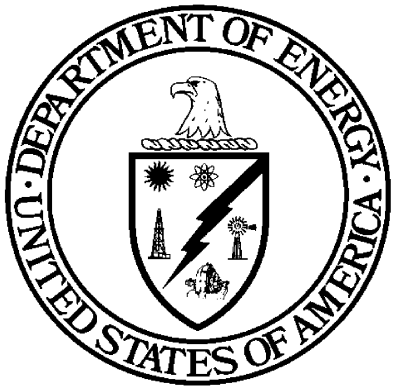
Search Print

DOE M 5632.1C-1

7-15-94
Change 1: 4-10-96

MANUAL FOR PROTECTION AND CONTROL OF SAFEGUARDS AND SECURITY INTERESTS



U.S. Department of Energy
Office of Security Affairs
Office of Safeguards and Security

DISTRIBUTION:
All Departmental Elements

INITIATED BY:
Office of Safeguards and Security

1. PURPOSE. This Manual provides detailed requirements to supplement DOE 5632.1C, PROTECTION AND CONTROL OF SAFEGUARDS AND SECURITY INTERESTS, which establishes policy for the protection and control of special nuclear material, Vital Equipment, classified matter, Departmental property and facilities, and unclassified irradiated reactor fuel in transit.

2. SUMMARY. This Manual is composed of 14 Chapters that provide detailed requirements for protection of safeguards and security interests. Chapter I addresses five essential ingredients for a successful program; site specific characteristics; design basis threat; strategy; planning; and graded protection. Chapters II through IV address protection and control of special nuclear material, classified matter, and unclassified irradiated reactor fuel in transit. Chapter V discusses Security Areas that are used to protect the safeguards and security interests discussed in Chapters II and III. The remaining chapters provide supporting information and requirements for effective implementation of safeguards and security programs.

3. REFERENCES AND DEFINITIONS. See Attachment 1.

4. DEVIATIONS. Deviations to this Manual shall be approved through procedures established in DOE 5630.11A, SAFEGUARDS AND SECURITY PROGRAM.

5. ASSISTANCE. Questions concerning this Manual should be directed to the Chief, Physical Security Branch, at 301-903-4244, or to the Classified Matter Protection and Control Program Manager, at 301-903-4805.

6. IMPLEMENTATION. The majority of requirements in this directive is the same as those contained in the superseded directives. Implementation Plans for any requirements that cannot be implemented within 6 months of the effective date of this Manual or within existing resources shall be developed by Heads of Field Elements and submitted to the Office of Safeguards and Security.

BY ORDER OF SECRETARY OF ENERGY:

ARCHER L. DURHAM
Assistant Secretary for
Human Resources and Administration

REFERENCES

1. Nuclear Waste Policy Act of 1982, Public Law 97-425, as amended.

2. Title 10 Code of Federal Regulations 73.37, "Requirements for Physical Protection of Irradiated Reactor Fuel in Transit," which identifies procedures for protection of licensee shipments of irradiated reactor fuel. Appendix D establishes training requirements for escorts of licensee shipments. Appendix E establishes levels of physical protection to be applied to international shipments.

3. Title 42 U.S.C. 2011, et seq., "Atomic Energy Act of 1954," as amended:

   a. Chapter 12, "Control of Information," sections 141-146, inclusive, which sets forth the principles for the control of Restricted Data.

   b. Chapter 18, "Enforcement," sections 221-233, which sets forth the authority necessary to protect Restricted Data and to protect property, and establishes criminal penalties for violation of provisions of the Atomic Energy Act.

   c. Chapter 18, "Enforcement," section 229, which sets forth the authority to issue regulations and establish penalties for violating these regulations relating to the entry upon or carrying, transporting, or otherwise introducing or causing to be introduced any dangerous weapon, explosive, or other dangerous instrument or material likely to produce substantial injury or damage to persons or property, into or upon any facility, installation, or real property of the DOE or NRC.

4. Title 42 U.S.C. 7270b, "Department of Energy Organization Act," which:

   a. Authorizes issuance of regulations concerning unauthorized: (1)entry into or upon the Strategic Petroleum Reserve, its storage or related facilities, or real property subject to the jurisdiction, administration, or in the custody of the Secretary of Energy under Part B of Title I of the Energy Policy and Conservation Act (42 U.S.C. 6231-6247); and (2) carrying, transporting, or otherwise introducing or causing to be introduced any dangerous weapon, explosive, or other dangerous instrument or material likely to produce substantial injury or damage to persons or property into or upon such property; and

   b. Provides that any person who willfully violates regulations issued under 42 U.S.C. 7270b is guilty of a misdemeanor, and shall be punished upon conviction by a fine of not more than $5,000, imprisonment of not more than 1 year, or both.

5. Title 10 CFR Part 710, "Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Significant Quantities of Special Nuclear Material," which establishes policies on personnel security clearances.

6. Title 10 CFR Part 860, "Trespassing on Administration Property," which is issued for the protection and security of facilities, installations, and real property subject to the jurisdiction or administration of, or in the custody of, DOE.

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

8. Title 14 CFR Part 108, "Airplane Operator Safety," which establishes a security program for scheduled passenger operations, public charter passenger operations, and persons on an aircraft or airport engaged in such operations.

9. Title 32 CFR Part 2001, "National Security Information," which sets the requirements for the classification of information.

10. Title 41 CFR Chapter 101, "Federal Property Management Regulations," which sets forth introductory material concerning the Federal Property Management Regulations System; its content; types; publications, including Federal specifications and standards; authority; applicability; numbering; deviation procedures; as well as agency consultation, implementation, and supplementation.

11. Title 48 CFR Section 952.204-2, "Security Requirements," which provides clauses to be included in contracts that involve or are likely to involve classified information, and section 952.245-2, Government Property (Fixed-Price Contracts), which includes clauses to be inserted in all contracts and modifications to contracts involving Government property.

12. Title 49 CFR 171-179, "Research and Special Programs Administration, Hazardous Materials Regulations," which identifies Federal rules for packaging and transporting hazardous materials, hazardous substances, and hazardous wastes, and section 173.22, "Shippers Responsibility," which describes physical protection requirements for the shipment of unclassified irradiated reactor fuel.

13. Executive Order 12356, "National Security Information," of 4-2-82, which provides requirements concerning classification of information.

14. Executive Order 12829, "National Industrial Security Program," of 1-6-93, which establishes a single, integrated, cohesive industrial security program to protect classified information and to preserve the Nation's economic and technological interests.

15. DOE 1240.2B, UNCLASSIFIED VISITS AND ASSIGNMENTS BY FOREIGN NATIONALS, of 8-21-92, which establishes authorities, responsibilities, and policy, and prescribes administrative procedures for visits and assignments by foreign nationals to DOE facilities.

16. DOE 1324.2A, RECORDS DISPOSITION, of 9-13-88, which establishes policies, procedures, standards, and guidelines for the orderly disposition of records.

17. DOE 1450.4, CONSENSUAL LISTENING-IN TO OR RECORDING TELEPHONE/RADIO CONVERSATIONS, of 11-12-92, which specifies the Department of Energy (DOE) policy regarding the consensual listening-in to or recording of conversations on radio and telephone systems.

18. DOE 1540.1A, MATERIALS TRANSPORTATION AND TRAFFIC MANAGEMENT, of 7-8-92, which establishes policies and procedures for transportation operations and traffic management.

19. DOE 1540.2, HAZARDOUS MATERIAL PACKAGING FOR TRANSPORT - ADMINISTRATIVE PROCEDURES, of 9-30-86, which establishes policies and procedures for approval of package designs for radioactive materials.

20. DOE 4300.1C, REAL PROPERTY MANAGEMENT, of 6-28-92, which establishes Departmental policies and procedures for planning the development and use of sites and facilities.

21. DOE 4330.4B, MAINTENANCE MANAGEMENT PROGRAM, of 2-10-94, which provides general policy and objectives for the management and performance of cost-effective maintenance and repair of property.

22. DOE 5000.3B, OCCURRENCE REPORTING AND PROCESSING OF OPERATIONS INFORMATION, of 1-19-93, which establishes a system for reporting operation information related to facilities and processing it to provide for the appropriate corrective action.

23. DOE 5300.3D, TELECOMMUNICATIONS: COMMUNICATIONS SECURITY, of 8-3-93, which establishes policy, responsibilities, and guidance concerning the communications security and automated information systems security aspects of telecommunications services of the Department of Energy.

24. DOE 5440.1E, NATIONAL ENVIRONMENTAL POLICY ACT COMPLIANCE PROGRAM, of 11-10-92, which establishes policies and procedures for implementing a DOE National Environmental Policy Act (NEPA) program.

25. DOE 5480.3, SAFETY REQUIREMENTS FOR THE PACKAGING AND TRANSPORTATION OF HAZARDOUS MATERIALS, HAZARDOUS SUBSTANCES, AND HAZARDOUS WASTES, of 7-9-85, which provides safety requirements for packaging and transporting hazardous materials, hazardous substances, and hazardous wastes.

26. DOE 5500.1B, EMERGENCY MANAGEMENT SYSTEM, of 4-30-91, which identifies overall policy and requirements for an emergency management system.

27. DOE 5500.3A, PLANNING AND PREPAREDNESS FOR OPERATIONAL EMERGENCIES, of 4-30-91, which establishes requirements for site-specific emergency plans and procedures for radiological emergencies (including malevolent threats or acts) occurring in Departmental reactor and non-reactor nuclear facilities.

28. DOE 5630.11A, SAFEGUARDS AND SECURITY PROGRAM, of 12-7-92, which provides policies for the safeguards and security program.

29. DOE 5630.14A, SAFEGUARDS AND SECURITY PROGRAM PLANNING, of 6-9-92, which establishes a standard approach to protection program planning.

30. DOE 5630.16A, SAFEGUARDS AND SECURITY ACCEPTANCE AND VALIDATION TESTING PROGRAM, of 6-3-93, which establishes a systematic process for demonstrating the adequacy and functional reliability of critical system elements.

31. DOE 5631.2C, PERSONNEL SECURITY PROGRAM, of 9-15-92, which establishes the policy, responsibilities, and authorities for implementing the DOE Personnel Security Program.

32. DOE 5631.4A, CONTROL OF CLASSIFIED VISITS, of 7-8-92, which establishes standards and procedures for controlling visitors to DOE and DOE contractor, subcontractor, and access permittee facilities.

33. DOE 5632.7A, PROTECTIVE FORCES, of 4-13-94, which prescribes Departmental policies and responsibilities for the protective force charged with the protection of safeguards and security interests.

34. DOE 5633.3A, CONTROL AND ACCOUNTABILITY OF NUCLEAR MATERIALS, of 2-12-93, which prescribes Departmental policies and responsibilities for control and accountability of nuclear materials.

35. DOE 5634.1B, FACILITY APPROVALS, SECURITY SURVEYS, AND NUCLEAR MATERIALS SURVEYS, of 9-15-92, which establishes Departmental requirements for onsite security and/or nuclear materials surveys of facilities with safeguards and security interests.

36. DOE 5639.1, INFORMATION SECURITY PROGRAM, of 10-19-92, which establishes the policies, procedures, and responsibilities for the protection and control of classified and sensitive information.

37. DOE 5639.5 TECHNICAL SURVEILLANCE COUNTERMEASURES PROGRAM, of 8-03-92, which establishes the Department's Technical Surveillance Countermeasures Program.

38. DOE 5639.6, CLASSIFIED COMPUTER SECURITY PROGRAM, of 9-15-92, which establishes requirements, policies, and responsibilities for the development and implementation of a Departmental program to ensure the security of information stored in classified computer systems.

39. DOE 5639.8A, SECURITY OF FOREIGN INTELLIGENCE INFORMATION AND SENSITIVE COMPARTMENTED INFORMATION FACILITIES, of 7-23-93, which establishes responsibilities and authorities for the protection of Foreign Intelligence Information and Sensitive Compartmented Information Facilities.

40. DOE 6430.1A, GENERAL DESIGN CRITERIA, of 4-6-89, which provides design criteria for use in the acquisition of the Department's facilities.

41. Access Delay, Technology Transfer Manual, SAND 87-1926/UC-515, Sandia National Laboratories, of 9-89, which defines the role of barriers in a physical protection program, provides a source for penetration times for barriers, and defines methods for upgrading existing barriers.

42. Alarm Communication and Display Technology Transfer Manual, SAND 90-0729/UC-515, Sandia National Laboratories, of 5-17-90, which provides a description of the hardware and techniques required to implement an alarm communication and display system.

43. American Society for Testing and Materials, "Standard Guide for Application of Radiation Monitors to the Control and Physical Security of Special Nuclear Material," C1112-93, which describes the state-of-the-art of radiation monitors in order to establish the context in which to write performance standards for monitors.

44. American Society for Testing and Materials, "Standard Practice for Design and Use of Ionizing Radiation Equipment for the Detection of Items Prohibited in Controlled Access Areas," F 792-88, which covers the use of ionizing radiation imaging techniques for the detection of questionable items such as weapons and devices intended to trigger explosives, in order to determine their presence in hand-carried baggage, packages, checked or unaccompanied luggage, cargo, or mail at screening points for controlling access to secure areas.

45. CGSS-2, Classification Guide for Safeguards and Security Information, of 6-90, Office of Classification and Technology Policy, which provides classification determinations for National Security Information (NSI) concerning nuclear safeguards and various aspects of security and guidance for classifying documents and materials containing NSI, Formerly Restricted Data, and/or Restricted Data.

46. Department of Transportation Advisory Circular 108-3, of 11-81, "Screening of Persons Carrying United States Classified Material," which delineates procedures for screening persons carrying classified matter on aircraft.

47. Department of Transportation OHMT-89.01, "Guidelines for Selecting Preferred Highway Routes for Highway Route Controlled Quantities of Radioactive Materials," of 1-89, which establishes Federal risk-assessment guidelines for the States to designate alternate routes.

48. "Design Basis Threat Policy for the Department of Energy (DOE) Programs and Facilities, (U)" of 7-28-93, issued by the Director of Security Affairs, which identifies and characterizes the range of potential adversary threats to the Department's programs and facilities, which could adversely impact national security, the health and safety of employees or the public, the environment, or DOE safeguards and security interests.

49. Director of Central Intelligence Directive (DCID) 1/7, "Security Controls on the Dissemination of Intelligence Information," of 1-7-84, which establishes policies, controls, and procedures for the dissemination and use of intelligence information and materials bearing the Director of Central Intelligence authorized control markings.

50. DCID 1/14, "Minimum Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information," of 11-27-84, which enhances the security protection of SCI through standards, procedures, security programs, and a facilitated security certification process among Department/agencies.

51. DCID 1/16, "Security Policy on Intelligence Information in Automated Systems and Networks," of 1-4-83, which establishes policies and procedures for the security of classified intelligence information processed or stored in automated systems and networks.

52. DCID 1/19, "Security Policy for Sensitive Compartmented Information," of 6-28-82, which establishes policies and procedures for the security, use, and dissemination of SCI.

53. DCID 1/20, "Security Policy Concerning Travel and Assignment of Personnel with Access to Sensitive Compartmented Information," of 3-11-85, which establishes the minimum policy concerning assignment and travel of U.S. Government civilian and military personnel, government consultants, and employees of government contractors who have, or who have had, access to SCI.

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

55. DCID 1/22, "Technical Surveillance Countermeasures," of 7-3-85, which establishes the policy and procedures for the conduct and coordination of technical surveillance countermeasures.

56. Entry Control Systems, Technology Transfer Manual, SAND 87-1927, Sandia National Laboratories, of 12-8-88, which provides a compilation of information regarding entry control systems and their application to physical protection programs.

57. Exterior Intrusion Detection Systems Technology Transfer Manual, SAND 89-1923/UC-515, Sandia National Laboratories, of 2-28-90, which provides a discussion of each class of detection systems and how to select the proper sensors and how to combine them into an effective perimeter subsystem.

58. Federal Specification W-A-450-C, "Alarm Systems Protective, Interior," which provides specifications for interior alarm systems.

59. Federal Specification AA-D-600B, "Door, Vault, Security," which provides specifications for vault doors.

60. Federal Specification AA-V-2737, "Modular Vault Systems," which describes a relocatable system for storing classified matter that provides a minimum of 15 minutes of protection against a multilevel tool attack, including torches, portable electric drills, power saws, hydraulic jacks, and other tools.

61. Federal Specification FF-L-2740, "Locks, Combination," which covers changeable, combination locks designed to be mounted on safes, security files, vault doors, and similar items.

62. Federal Specification FF-P-110, "Padlock, Changeable Combination," which covers changeable combination locks intended for use as determined for low level resistance to forced entry and high level manipulation or surreptitious action.

63. Federal Specification FF-P-2827, "Padlock, Key Operated, General Field Service," which describes two sizes of "U"-shaped shackle, key-operated, heavy-duty commercial padlocks.

64. General Records Schedule 18, "Security and Protective Service Records," of June 1988, National Archives and Records Administration.

65. Military Specification MIL-L-15596G, "Locks, Combination for General Services Administration-Approved Security Containers, Vault Doors, and Safe Lockers," which covered commercially available combination locks bearing the Underwriters Laboratory label for Groups 1 and 1R as defined in UL 768, and was cancelled on 5-5-93.

66. Military Specification MIL-P-17802, which covers key-operated, pin tumbler, dead-bolt padlocks, and padlock sets for military use.

67. Military Specification MIL-P-43607G, "Padlock, Key Operated, High Security, shrouded Shackle," which covers one type of key-operated, high-security, shrouded shackle padlock that employs a dead bolt locking mechanism.

68. Protecting Security Communications, Technology Transfer Manual, SAND 90-0397/UC-515, Sandia National Laboratories, of 1-90, which provides a discussion of the functions of a security communications network, its susceptibility to disruption, and the means by which security radio communications may be protected.

69. Safeguards and Security Definitions Guide, Office of Safeguards and Security, of 12-20-93, which contains standardized definitions of terms used in the Safeguards and Security Program.

70. Underwriters Laboratories-365, "Police Station Connected Burglar Alarm Systems and Units," which states requirements covering construction, performance, and maintenance of police station connected burglar alarm units and systems.

71. Underwriters Laboratories (UL) Standard 752, "Standard for Bullet-Resisting Equipment," which provides a standard for bullet-resisting equipment.

72. Video Assessment Technology Transfer Manual, SAND 89-1924/UC-515, Sandia National Laboratories, of 8-21-89, which provides a compilation of information regarding video assessment systems used in physical protection programs.

73. Volume 50 FR 46452, of 11-18-85, "Federal Radiological Emergency Response Plan," Federal agency responsibilities during peacetime radiological emergencies including those in transportation.

DEFINITIONS

Definitions of terms commonly used in the Safeguards and Security Program are provided in the "Safeguards and Security Definitions Guide," which is maintained and distributed by the Office of Safeguards and Security.

TABLE OF CONTENTS

CHAPTER V
SECURITY AND RESTRICTED ACCESS AREAS

CHAPTER VI
PROTECTION ELEMENT:INTRUSION DETECTION AND ASSESSMENT SYSTEMS

CHAPTER VII
PROTECTION ELEMENT: ACCESS CONTROL AND ENTRY/EXIT INSPECTIONS

CHAPTER VIII
PROTECTION ELEMENT: BARRIERS AND LOCKS

CHAPTER IX
PROTECTION ELEMENT: SECURE STORAGE

CHAPTER X
PROTECTION ELEMENT: COMMUNICATIONS

CHAPTER XI
RESERVED

CHAPTER XII
PROTECTION ELEMENT: MAINTENANCE

CHAPTER XIII
PROTECTION ELEMENT: POSTING NOTICES

CHAPTER XIV
PROTECTION ELEMENT: SECURITY BADGES AND CREDENTIALS

Vertical line denotes change.

CHAPTER I

PROTECTION AND CONTROL PLANNING

1. SITE-SPECIFIC CHARACTERISTICS. Protection programs shall be tailored to address specific site characteristics and requirements, current technology, ongoing programs, operational needs, and to achieve acceptable protection levels that reduce inherent risks on a cost-effective basis.

2. THREAT. The "Design Basis Threat Policy for the Department of Energy (DOE) Programs and Facilities (U)" shall be used in conjunction with local threat guidance and vulnerability assessments for protection and control program planning.

3. PROTECTION STRATEGY.

   a. Strategies for the physical protection of special nuclear material and Vital Equipment shall incorporate the applicable requirements established in Chapter II. Protection strategy may be graduated to address varying circumstances and may range from denial to containment to recapture/recovery to pursuit.

      (1) A denial strategy shall be used for the protection of a safeguards and security interest (e.g., Category IA special nuclear material, certain radiological sabotage targets) where unauthorized access presents an unacceptable risk. Programs shall be designed to prevent unauthorized control; i.e., an unauthorized opportunity to initiate or credibly threaten to initiate a nuclear dispersal or detonation, or to use available nuclear materials for onsite assembly of an improvised nuclear device.

      (2) A containment strategy shall be used to prevent the unauthorized removal of Category II or greater special nuclear material.

      (3) Should denial and/or containment referenced in (1) and (2) above fail, a recapture/recovery or pursuit strategy would then be required. Forces capable of rapid reaction are vital to the implementation of recapture or recovery contingencies.

      (4) Programs must be designed to mitigate the consequences of acts of radiological/toxicological sabotage that would cause unacceptable impact to national security or pose significant dangers to the health and safety of employees, the public, or the environment.

   b. Strategies for the protection and control of classified matter shall incorporate the applicable requirements established in Chapter III. In addressing the threat to the Department's information assets, emphasis must be placed on security systems that will detect or deter unauthorized disclosure or modification or the loss of availability of classified and sensitive, but unclassified, information and its unauthorized removal from a site or facility.

   c. Security countermeasures to address bombings shall consider a range of activities from handcarried, mailed, and vehicle-transported devices.

d. Programs shall be designed to prevent radiological/toxicological sabotage acts that would cause unacceptable impact to national security or pose significant dangers to the health and safety of employees, the public, or the environment, and/or to mitigate the consequences of such acts that might occur.

e. Safeguards and security systems and critical systems elements shall be performance tested to ascertain their effectiveness in providing countermeasures to address design basis threats.

4. PLANNING.

a. Site Safeguards and Security Plans. The details of site protection measures shall be addressed in the Site Safeguards and Security Plan, as required by DOE 5630.14A, SAFEGUARDS AND SECURITY PROGRAM PLANNING.

b. Security Plans. At locations where a Site Safeguards and Security Plan is not required due to the limited scope of safeguards and security interests, a security plan shall be developed to describe the protection program in place.

5. GRADED PROTECTION. By graded approach, DOE intends that, in the development and implementation of protection and control programs, the level of effort and magnitude of resources expended for the protection of a particular security interest are commensurate with the security interest's importance or the impact of its loss, destruction, or misuse. Interests whose loss, theft, compromise, and/or unauthorized use will have serious impact on the national security, and/or the health and safety of DOE and contractor employees, the public, the environment, or Department of Energy programs, shall be given the highest level of protection. For example, use of a weapon of mass destruction by a terrorist(s) could have consequences so grave as to demand the highest reasonably attainable standard of security. Protection of other interests shall be graded accordingly. Asset valuation, threat analysis, and vulnerability assessments shall be considered, along with the acceptable level of risk and any uncertainties, to decide how great is the risk and what protection measures are to be applied. Heads of Departmental Elements shall provide a rational, cost-effective, and enduring protection framework using risk management as the underlying basis for making security-related decisions. It should be recognized that risks will be accepted, i.e., that actions cannot be taken to reduce the potential for or consequences of all malevolent events to zero; however, an acceptable level of risk will be determined based on evaluation of a variety of facility-specific goals and considerations. Protection-related plans shall describe, justify, and document the graded protection provided the various safeguards and security interests.

CHAPTER II

PROTECTION OF SPECIAL NUCLEAR MATERIAL AND VITAL EQUIPMENT

1. GENERAL. This chapter outlines requirements for the protection of Categories I through IV quantities of special nuclear material and Vital Equipment. The following requirements shall apply:

   a. A facility shall not receive, process, transmit, or store special nuclear material until that facility has been approved as required by DOE 5634.1B, FACILITY APPROVALS, SECURITY SURVEYS, AND NUCLEAR MATERIALS SURVEYS.

   b. Nuclear material production reactors and fuel shall be protected consistent with the category of special nuclear material involved and/or the consequences of radiological sabotage.

   c. Protection afforded special nuclear material shall be graded according to the nuclear material safeguards category, as defined in Figure I-2 of DOE 5633.3A, CONTROL AND ACCOUNTABILITY OF NUCLEAR MATERIALS, and shall reflect the specific nature of special nuclear material existing at each site. DOE 5633.3A shall be used to determine if there is a potential to accumulate a category quantity of special nuclear material by theft of material from more than one location (rollup).

   d. Factors, such as ease of separability, accessibility, and concealment; quantity, chemical form, isotopic composition, purity, and containment; portability; protection strategies; radioactivity; and self-protecting features, shall be considered in determining physical protection systems for each category of special nuclear material.

   e. When special nuclear material is classified because of its configuration or content, or because it is part of a classified item, it shall receive the physical protection required by the highest level of classification of the configuration, content, or item, or category of special nuclear material involved, whichever is greater.

   f. Protective force personnel, as determined by a vulnerability assessment and documented in the Site Safeguards and Security Plan, shall be available and positioned to respond to a verified threat occurrence to contain, interrupt, and/or neutralize adversaries within the required response times.

   g. Intrusion detection shall be accomplished through a combination of intrusion sensors and tamper-indicating devices, material surveillance procedures, material accounting and tracking, and/or specialized nuclear measurement techniques.

h. Delay mechanisms shall be employed to prevent removal or unauthorized use of Category I and II quantities of special nuclear material. Delay mechanisms may include passive barriers (e.g., walls, ceilings, floors, windows, doors, security bars), activated barriers (e.g., sticky foam, popup barriers), and visual obscurants (e.g., cold smoke).

i. Specific protection requirements, such as systems and protective personnel response capabilities necessary to satisfy identified protection needs, shall be documented.

2. ACCESS. Access controls shall be in place to ensure that only properly cleared and authorized personnel are permitted unescorted access to special nuclear material and Vital Equipment. Access authorizations (security clearances) shall be accomplished according to DOE 5631.2C, PERSONNEL SECURITY PROGRAM. See Table II-1 for access authorization required for special nuclear materials. Access authorization requirements for Vital Equipment shall be comparable to Category I special nuclear material.

3. PROTECTIVE FORCE POSTS. See DOE 5632.7A, page VI-6, paragraph 2.

4. STORAGE. Each facility shall have controls for nuclear materials held in storage (see Chapter IX for elaboration) consistent with the graded safeguards concept. Controls for storage shall:

a. Be formally documented;

b. Assure that only authorized personnel have access to the storage repositories (see Chapter VII);

c. Prevent and/or detect unauthorized access;

d. Describe procedures used to authenticate material movements into or out of a repository;

e. Include procedures for investigating and reporting abnormal conditions;

f. Provide a record system to document ingress/egress to repositories; and

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

5. CATEGORY I QUANTITIES OF SPECIAL NUCLEAR MATERIAL.

a. In Process. Material shall be used or processed within Material Access Areas. DOE 5633.3A, page III-3, paragraph 3b(1) requires a material surveillance program to detect unauthorized material flows and transfers. Any location within a Material Access Area that contains unattended Category I quantities of special nuclear material in use or process shall be equipped with intrusion detection systems or other effective means of detection approved by the cognizant local Departmental authority for safeguards and security.

SPECIAL NUCLEAR MATERIAL CATEGORY	MINIMUM LEVEL OF ACCESS AUTHORIZATION REQUIRED	REMARKS
I	Q	Hands-on access or transporation of Category I quantities of SNM may require additional measures, such as Personnel Security Assurance Program participation and/or enhanced material surveillance procedures, to further reduce the probability of insides acts.
II with credible rollup to I	Q	
II and III	L	Unless special circumstances deremined by site vulnerability assessment require Q access authorization to minimize risk. Document in Site Safeguards and Security Plan.
IV	None	Unless special circumstances determined by site vulnerability assessment require access authorization to mitigate risk. Document in Site Safeguards and Security Plan.

TABLE II-1
ACCESS AUTHORIZATION REQUIREMENTS

b. Storage. Material shall be stored within a Material Access Area.

(1) When not in process or when unattended, material falling under Attractiveness Level A shall be stored in a vault. Storage facilities for Category I special nuclear material Attractiveness Level A, constructed after the date of this Manual, shall be underground or below-grade construction.

(2) Material falling under Attractiveness level B shall be stored in a vault or be provided enhanced protection that exceeds vault-type room storage (e.g., collocated protective force response station and/or activated barrier(s)).

(3) Material falling under Attractiveness Level C shall, as a minimum, be stored in a vault-type room.

c. In-Transit. Protection requirements for material in transit shall be as follows:

(1) Domestic offsite shipments of Category I quantities of special nuclear material shall be made by the Transportation Safeguards System, operated under the auspices of the Albuquerque Operations Office.

(2) Packages or containers containing special nuclear material shall be sealed with tamper-indicating devices.

(3) Protection measures for movements of material between Protected Areas at the same site, or between Protected Areas and staging areas at the same site, shall be under direct surveillance by the number of Security Police Officers necessary to protect against threats as established in the Department's threat policy (See paragraph 3, page I-1).

6. CATEGORY II QUANTITIES OF SPECIAL NUCLEAR MATERIAL.

a. In Process. Material shall be used or stored only within a Protected Area. All such matter shall be under material surveillance procedures.

b. Storage. When not in process or when unattended, material shall be stored in a vault or a vault-type room located within a Protected Area.

c. In Transit. Shipments shall conform to the shipment requirements for Category I quantities of special nuclear material (See paragraph 4c above).

7. CATEGORY III QUANTITIES OF SPECIAL NUCLEAR MATERIAL.

a. In Process. Category III quantities of special nuclear material shall be processed within a Security Area that provides, at a minimum, the protection of a Limited Area.

b. Storage. When not in process or when unattended, material shall be stored, at a minimum, within a Limited Area and secured within a locked security container locked room. The container or locked room containing the matter shall be under the protection of an intrusion detection system or protective patrol at intervals not to exceed 8 hours.

c. In Transit.

(1) Domestic offsite shipments of classified configurations of Category III quantities of special nuclear material may be made by Transportation Safeguards System.

(2) Methods of shipping unclassified configurations:

(a) Truck or Train. Truck or train shipments shall meet the following requirements:

1 Government-owned or exclusive-use truck, commercial carrier, or rail may be used to ship Category III quantities of special nuclear material.

2 A detailed inspection of the transport vehicle shall be conducted before loading and shipment. Cargo compartments shall be locked and sealed while en route.

3 Personnel assigned to escort shipments shall maintain periodic communication with a control station operator who can request appropriate local law enforcement agency response, if needed.

4 Shipments shall be made without intermediate stops except for emergency reasons, driver relief, meals, refueling, or transfer of cargo.

(b) Air Shipment. Air shipments of Category III quantities of special nuclear material may take place if not otherwise prohibited by statute or otherwise limited by implementing instructions. The shipments shall be under the direct observation of the authorized escorts during all land movements and loading and unloading operations.

(3) Movements of Category III quantities of special nuclear material between Security Areas at the same site shall be according to the appropriate locally-developed security plan.

8. CATEGORY IV QUANTITIES OF SPECIAL NUCLEAR MATERIAL.

a. Processing and Storage. Material shall be in a locked area when not in use, and shall be received, processed, and stored according to procedures approved by the cognizant local Departmental authority for safeguards and security.

b. In Transit.

(1) Domestic offsite shipments of classified configurations of Category IV quantities of special nuclear material may be made by means of the Transportation Safeguards System, under procedures approved by the Albuquerque Operations Office as deemed appropriate, and by agreements between the Manager, Albuquerque Operations Office, and the respective Heads of Field Elements.

(2) Shipments of unclassified configurations of material may be made by truck, rail, or water, in commercial, for-hire, or leased vehicles. If not otherwise prohibited by State or Federal laws, Category IV quantities of special nuclear material may also be shipped by air.

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

(b) Shipper shall be required to give the consignee an estimated time of arrival before dispatch, and followup with a written confirmation not later than 48 hours after dispatch.

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

9. VITAL EQUIPMENT. Site Safeguards and Security Plans shall define applicable threats and measures to protect Vital Equipment from hostile actions.

CHAPTER III

PROTECTION AND CONTROL OF CLASSIFIED MATTER

1. GENERAL.

   a. Classification levels shall be used in determining the degree of protection and control required for classified matter.

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

   c. Custodians and authorized users of classified matter are responsible for the protection and control of such matter.

   d. Buildings and rooms containing classified matter shall be afforded the security measures necessary to prevent unauthorized persons from gaining access to classified matter, specifically to include security measures to prevent persons outside the facility protective zone from viewing or hearing classified information. Conference rooms and areas specifically designated for classified discussions shall follow Technical Surveillance Countermeasures Program requirements.

   e. Sensitive Compartmented Information Facilities shall be afforded physical protection in accordance with the Director of Central Intelligence Directives (see Attachment 1). Any matters pertaining to this subject shall be referred to the Director of Safeguards and Security for coordination.

2. IN USE. Classified matter in use shall be constantly attended by or under the control of a person or persons having the proper access authorization and a need-to-know, who are responsible for its protection. (Exception: Local safeguard and security authorities may establish written local policy, addressing operational needs, that allows Confidential and/or Secret matter to be left temporally unattended within an appropriately locked room, within an attended Limited Area, Protected Area, or Exclusion Area, during normal working hours. The period of time shall not exceed 2 hours. Unattended within a locked room for up to 2 hour periods in such cases is considered "In Use".)

3. IN STORAGE.

   a. General. Classified matter shall be stored in a manner to prevent unauthorized persons from gaining access.

   b. Restrictions on Use of Security Containers.

      (1) Funds, firearms, medical items, controlled substances, precious metals, or other items susceptible to theft shall not be stored in the same security container that is used to store classified matter.

(2) Security containers shall not bear any external classification or other type markings that would indicate the level of classified matter authorized to be stored within the container. For identification purposes, each security container shall externally bear an assigned number.

c. Requirements. Security containers required for the storage of classified matter shall, as a minimum, conform to the applicable requirements of Chapter IX of this Manual. Classified matter that is not under the personal control of an authorized person shall be stored as prescribed below.

(1) Top Secret Matter. Top Secret matter shall be stored in a locked, General Services Administration-approved security container. The security container shall be located within a Security Area providing as a minimum the protection level of a Limited Area. In addition, the security container shall be under intrusion detection alarm protection or protective patrol, with inspections on a 4-hour basis.

(2) Secret Matter. Secret matter shall be stored in a manner authorized for Top Secret matter or in one of the following ways:

(a) In a locked General Services Administration approved security container.

1 General Services Administration-approved security containers not located within the minimum protection level of a Limited Security Area shall be under intrusion detection alarm protection.

2 Steel filing cabinets, not meeting General Services Administration requirements, but approved for use prior to the date of this Manual, may continue to be used until there is a need for replacement. They shall be equipped with a minimum of an Underwriter Laboratories Group 1R, built-in, changeable combination lock. Steel filing cabinets located within the minimum protection level of a Limited Security Area shall be under intrusion detection alarm protection or protective patrol on an 8-hour basis. If the steel filing cabinet is not located within a minimum protection level of a Limited Security Area, it shall be under intrusion detection alarm protection.

3 In open storage or in unlocked cabinets within a locked vault or vault-type room.

(b) Material whose size, weight, or construction offers substantial resistance to unauthorized removal or surreptitious access to contents shall be stored within the minimum protection level of a Limited Security Area in one of the following ways:

1 Within a locked building, or in a locked room within a building. The building or room shall provide visible evidence that an intruder has attempted to penetrate or has penetrated the building or room. In addition, the room or building shall be under intrusion detection alarm protection or subject to protective patrols on an 8-hour basis.

2 In open storage within a securely locked and separately fenced area. The classified items, as appropriate, shall be concealed from unauthorized view, and the storage area shall be intrusion detection alarm protected or subject to protective patrols on a 4-hour basis.

3 In open storage without a separately fenced and locked area. The classified matter shall be concealed from unauthorized view. The storage location shall be under intrusion detection alarm protection or subject to protective patrols on a 2-hour basis.

(c) Material whose size, weight, or construction offers substantial resistance to unauthorized removal, but nevertheless is susceptible to unauthorized removal or surreptitious access shall be protected in the manner set forth in subparagraphs 3c(2)(b) 1, 2, or 3 above, except that protective patrols shall occur at intervals not to exceed 2 hours.

(3) Confidential Matter. Confidential matter shall be stored in a manner authorized for Secret matter or in one of the following ways:

(a) In a locked, General Services Administration-approved security container or steel filing cabinet. Steel filing cabinets shall be equipped with a minimum of an Underwriters Laboratories Group 1R, built-in, changeable combination lock, or lock bar with combination padlock that meets Federal Specification FF-P-110 "Padlock, Changeable Combination." If the steel filing cabinet is not located within the minimum protection level of a Limited Area or Exclusion Area, then it shall be under central alarm station protection.

(b) Time intervals for the protective personnel patrols referenced in subparagraphs 3c(2)(b) 1, 2, and 3 above shall be changed to 24, 12, and 6 hours respectively for Confidential matter.

d. Protective Personnel.

(1) In the event that an unattended repository or location containing classified matter is found open, the repository shall be secured by designated protective personnel and a custodian shall be notified immediately. The contents shall be checked no later than the next workday. If there is an indication of a violation or compromise, the contents shall be checked immediately by a custodian, being careful not to destroy fingerprints or other physical evidence. Report as required by DOE 5639.1, INFORMATION SECURITY PROGRAM, and DOE 5000.3B, OCCURRENCE REPORTING AND PROCESSING OF OPERATIONS INFORMATION. Refer to DOE 5639.1 regarding the conduct of preliminary inquiries.

(2) Response to intrusion detection alarms shall be by protective personnel, private security firms, or local law enforcement personnel, as documented in approved security plans.

e. Alternate Storage Locations.

(1) With prior written Departmental approval, a bank safe deposit box/vault may be used for storage of Secret or Confidential matter, provided that the lock and keys to the box/vault are changed prior to such use and the customer's key is furnished only to persons authorized access to the contents.

(2) Federal Records Centers approved as outlined in DOE 5634.1B may be used for the storage of classified information.

4. MARKING. Within 6 months of the date of this Order the following requirements shall be fully implemented. Classified matter marked according to previous requirements need not be remarked to conform with the following requirements. Classified matter must clearly indicate the classification level (and category if RD or FRD).

a. General. Classified matter must be properly and fully marked to indicate the classification level (and category if Restricted Data (RD) or Formerly Restricted Data (FRD)) and any other required notations. Specific examples of markings, including their use, format, and placement are contained in "The Guide for Implementation of CLASSIFIED MATTER PROTECTION AND CONTROL."

b. Originator Identification. Classified documents shall be marked to show the name of the organization responsible for its preparation and the date of preparation.

c. Classification Level. The overall classification level of a document shall be marked on the outside of the front cover (if any), on the title page (if any), on the first page, and on the outside of the back cover or last page. These markings shall be clearly distinguishable from the informational text. Classified material shall have classification level stamped, printed, etched, written, engraved, painted, or affixed by means of a tag, sticker, decal, or similar device. When marking is not practical, written notification of the markings shall be furnished to recipients. The highest classification level of each page shall be marked at the top and bottom of interior pages of classified documents; or when individual page marking is not feasible, the overall classification level of the document may be used instead. These markings shall be clearly distinguishable from the informational text.

d. Classification Category. Documents containing RD or FRD must be marked in the following manner: the overall classification category shall be marked on the outside of the front cover (if any), on the title page (if any), and on the first page. Classified material shall have classification category stamped, printed, etched, written, engraved, painted, or affixed by means of a tag, sticker, decal, or similar device. When marking is not practical, written notification of the markings shall be furnished to recipients. These markings shall be clearly distinguishable from the informational text.

e. Components. When components of a document are to be used separately, each major component shall be marked as a separate document. Components include: annexes or appendices, attachments to a letter, and major sections of a report. If an entire major component is unclassified, "UNCLASSIFIED" may be marked at the top and bottom of the first page and a statement included, such as: "All portions of this (annex, appendix, etc.) are UNCLASSIFIED." When this method of marking is used, no further markings are required on the unclassified component.

f. Portions.

(1) For National Security Information (NSI) classified by an Original Classifier each section, part, paragraph, or similar portion of a classified document shall be marked to show the classification level or be identified as unclassified. In marking portions, the symbols (TS) for TOP SECRET, (S) for SECRET, (C) for CONFIDENTIAL, and (U) for UNCLASSIFIED shall be used. Classification levels of portions of a document shall be shown by the appropriate classification symbol placed immediately following the portion's letter or number, or in the absence of letters or numbers, immediately before the beginning of the portion.

(2) Documents containing RD or FRD are not required to be portion marked.

(3) Portions of U.S. documents containing foreign government information shall be marked to reflect the foreign country of origin as well as the appropriate classification level, for example, (U.K.-C indicating United Kingdom - Confidential).

(4) Portions of U.S. documents containing NATO information shall indicate NATO or COSMIC, including the appropriate classification level, for example, (NATO-S) or (COSMIC-TS).

(5) If portion marking is appropriate for Foreign Government Information this notice may be abbreviated as "FGI."

g. Subjects and Titles. Except for extraordinary circumstances, unclassified subjects and titles shall be used for classified documents. Subjects or titles shall be marked with the appropriate classification level (and classification category if RD or FRD), for example, (U), for unclassified titles or subjects and, when necessary, (TS), (S), or (C) for classified titles or subjects. The symbols shall be placed immediately following the title or subject.

h. Classifier Information. DOE 5650.2B, IDENTIFICATION OF CLASSIFIED INFORMATION, specifies the classifier information that must be contained on classified matter. These include:

(1) Date of classification.

(2) Name, position title, and organization of the Authorized Classifier.

(3) Designation of the guide or source document, if derivatively classified (NSI) only; and

(4) Duration of classification (NSI only).

i. Top Secret Destruction Date. When upon origination or reproduction it is determined that TOP SECRET matter shall be destroyed at a particular time, the classifier shall note this fact on all copies except record copies.

j. Caveats. In addition to the markings specified above, as appropriate, classified matter shall be marked with caveats as indicated below:

(1) Dissemination and Reproduction Notices. When programmatic requirements require special dissemination or reproduction limitations on classified information the following notation shall be used:

(a) "FURTHER DISSEMINATION ONLY AS AUTHORIZED BY GOVERNMENT AGENCY" apply to documents whose further dissemination within the receiving contractor facility is restricted to persons authorized by the addressee. Dissemination outside the facility is prohibited without the approval of the contracting activity.

(b) "REPRODUCTION REQUIRES APPROVAL OF ORIGINATOR" apply to documents that may not be reproduced without the specific, written approval of the originator.

(2) Foreign Government Information. The notice "FOREIGN GOVERNMENT INFORMATION" is used on U.S. documents to ensure that information of foreign origin is not declassified prematurely or made accessible to nationals of a third country without the consent of the originator.

(3) North Atlantic Treaty Organization (NATO) Information.

(a) NATO CLASSIFIED. NATO has four levels of classified information: COSMIC TOP SECRET (CTS), NATO SECRET (NS), NATO CONFIDENTIAL (NC), and NATO RESTRICTED (NR). When "North Atlantic Treaty Organization (NATO)" or "COSMIC" precedes a classification information is the property of NATO.

(b) NATO UNCLASSIFIED (NU). This marking, applied to NATO information that does not require security protection, is handled in accordance with information management procedures.

(c) ATOMAL. Another category of NATO information is called ATOMAL. This category is either U.S. Restricted Data or Formerly Restricted Data or United Kingdom Atomic Information that has been officially released to NATO. ATOMAL information is classified either COSMIC TOP SECRET ATOMAL (CTSA), NATO SECRET ATOMAL (NSA), or NATO CONFIDENTIAL ATOMAL (NCA), depending upon the damage that would result from unauthorized disclosure.

(4) Director of Central Intelligence Information. The following are markings authorized for use only by the intelligence community for intelligence information:

(a) No Dissemination to Contractors (NOCONTRACT). This marking indicates that the information contained in the document must not be released to contractors or consultants without the permission of the originating agency.

(b) No Foreign Dissemination (NOFORN). This marking indicates that the information contained in the document must not be released to foreign nationals or any parties representing foreign interests, nor shall it be released to members of the public because this is considered to be tantamount to foreign disclosure.

(c) Originator Controlled (ORCON). This marking indicates that the document bearing the marking is controlled by the originator. Reproduction or redistribution of such documents require the permission of the originator.

(d) Proprietary Information (PROPIN). This marking indicates that the information contained in the document must not be released in any form to an individual, organization, or foreign government that has any interests, actual or potential, in competition with the source of the information, without the permission of the originating agency.

(e) REL (Authorized for Release to Country). This marking applies to classified intelligence an originator has predetermined to be releasable or has released through established foreign disclosure procedures and channels to a specified foreign country(ies), or international organization(s).

(f) Warning Notice--Intelligence Sources and Methods (WNINTEL). This marking applies to documents containing information relating to intelligence sources or methods.

(5) Weapon Data. The following are markings associated with atomic weapons or nuclear explosive devices:

(a) Sigma Category. This marking refers to Restricted Data and Formerly Restricted Data specifically defined in ten separate categories (1-5 and 9-13) concerning the design, manufacture, or use of atomic weapons or nuclear explosive devices.

(b) Critical Nuclear Weapons Design Information (CNWDI). A Department of Defense marking designating TOP SECRET or SECRET Restricted Data revealing the theory of operation or design of the components of a thermonuclear or implosion-type fission bomb, warhead, demolition munitions, or test device.

(c) Sensitive Use Control Information (SUCI). This marking refers to classified matter containing information, the knowledge of which would significantly enhance an adversary's ability to circumvent a weapon's use control features.

k. Remarking Downgraded/Declassified Matter. Matter marked for automatic downgrading or declassification may be downgraded, or declassified and remarked accordingly. Matter not marked for automatic downgrading or declassification will remain classified until a determination is made by the originating agency.

l. Marking Special Documents. The following are specific placement requirements for markings identified above:

(1) Charts, Maps, Drawings, and Tracings. The overall classification level of the document shall be marked under the legend, title, or scale block. Classification markings shall be visible when charts, maps, drawings, or tracings are folded or rolled.

(2) Messages. The overall classification level (and category if RD or FRD) of the message shall be the first item of information in the text. When messages are printed by an automated system, markings may be applied by that system, provided the markings are clearly distinguishable from the informational text. If applicable, downgrading instructions shall be included on the last line of text and may be abbreviated as follows:

DNG/S or C (date or event); or
DECL (date or event).

(3) Microforms. Microforms contain images or text in sizes too small to be read by the unaided eye. Markings specified by this chapter shall be marked on the medium or its container, to be readable by the unaided eye. These markings shall also be included on the image. Markings shall consider the media involved.

(4) Motion Picture Films or Video Tapes. Classified motion picture films and video tapes shall be marked at the beginning and end of each reel. Such markings shall be visible when projected or viewed.

(5) Photographs. Roll negatives or positives shall be marked at the beginning and end of each strip. Prints and reproductions shall show these markings on the face side of the print, if possible. When this is not possible, the marking shall be applied to the reverse side, or affixed by pressure tape label, staple strip, or other comparable means. When self-processing film or paper is used to photograph or reproduce classified information, if all parts of the last exposure have not been removed from the camera the camera shall be protected at the classification level (and category if RD or FRD) of information contained on the media.

(6) Transparencies, Slides, and Sheet-Film. Classification level and category shall be shown on the image of the first transparency, slide, sheet film of a series. All other applicable markings specified in this chapter shall be shown on the border or frame, or in the accompanying documentation. The succeeding transparencies, slides, and sheet film must indicate classification level only. When a set of transparencies, slides, or sheet film is handled and controlled as a single document, only the title slide or transparency requires the other applicable markings.

(7) Recordings. Magnetic, electronic, or sound recordings shall indicate the overall classification level (and category if RD or FRD) at the beginning and end of the recording.

(8) Automated Information Systems Media. Specific requirements for the handling of automated information system media are addressed in DOE 5639.6, CLASSIFIED COMPUTER SECURITY PROGRAM.

(9) Translations. U.S. classified information translated into a foreign language shall be marked as U.S. classified information, and show the equivalent foreign government classification.

(10) Radiographs and X-rays. When standard markings are not practical on the radiograph or x-ray, they shall be placed on the jacket, folder, or similar covering. The user must ensure that the appropriately marked jacket, folder, or covering remains with the associated radiograph or x-ray.

m. File Folders and Other Containers. When not in approved security containers, file folders and other items containing classified documents shall be marked to indicate conspicuously the highest classification level of any classified matter included.

n. Transmittal Documents. The first page of a transmittal document shall be marked with the highest level of classified information being transmitted, and with an appropriate notation to indicate its classification when the enclosures are removed. Additional markings (including category if RD or FRD) from the enclosure shall be included on transmittal documents when they convey restrictions.

o. Working Papers and Drafts. Classified working papers and drafts are considered to be interim production stages toward the generation of a permanent document. Working papers need only contain the following markings:

(1) Date when created;

(2) Highest classification level (and category if RD or FRD) of any information contained therein;

(3) Those prescribed for a finished document of the same classification when:

(a) Released by the originator outside the activity,

(b) Retained for more than 180 days from the date of origin, or

(c) Filed permanently.

p. Miscellaneous. Typewriter ribbon cartridges and spools or carbons must be marked with the appropriate classification level and protected accordingly until destroyed. No additional markings are required.

q. Other Agency and Foreign Government Documents Not Conforming to DOE Requirements. Documents received from other agencies and foreign governments not marked to conform to DOE requirements need not be remarked. However, as a minimum, all documents received must indicate a classification level (and category if RD or FRD).

r. Cover Sheets. The Standard Form (SF) cover sheet shall be applied to classified documents when removed from a security container. Contractors may use locally developed cover sheets of the same color and format as the standard forms. SF 703 is the TOP SECRET cover sheet, SF 704 is the SECRET cover sheet, and SF 705 is the CONFIDENTIAL cover sheet. In lieu of standard forms, a National Security Council cover sheet shall be affixed to each copy of a document containing classified National Security Council information.

5. ACCOUNTABILITY AND CONTROL SYSTEMS.

a. General. Departmental Elements and covered contractors shall establish control systems to prevent unauthorized access to classified information. Accountability systems provide a system of procedures which provide an audit trail. Accountable matter includes TOP SECRET matter, SECRET matter that is maintained (e.g., used, processed, stored) outside of Limited Areas, Exclusion Areas, or Protected Areas, and any matter that requires accountability by National, International, or programmatic requirements.

b. Control Stations. Departmental Elements and covered contractors shall establish control stations to maintain records and control classified matter received by and/or dispatched from their facilities. Employees must be designated and trained to operate these control station(s) and the employees shall have access authorizations commensurate with the level of their classified control responsibilities. TOP SECRET Control Officers shall function as control stations for TOP SECRET matter.

c. Top Secret Access Records. An up-to-date record (i.e., DOE Form 5635.4, "Top Secret Access Sheet") shall be maintained of all persons who are authorized access (including visual or aural access) to TOP SECRET information. The record shall identify the item of TOP SECRET matter, show the name of each individual given access, and the date (or inclusive dates) of access. For employees whose duties require knowledge of the combination of containers holding TOP SECRET matter, the SF 700 is the only access record that needs to be retained for the combination.

d. Accountability Records. Control station operators shall maintain accountability systems for accountable matter. As a minimum accountability records shall indicate for each accountable item:

(1) Date of the matter;

(2) Originating activity;

(3) Activity from which the matter was received, if applicable;

(4) Date of receipt, if applicable;

(5) Classification level (and category if RD or FRD), and additional handling caveats, if any, of the matter;

(6) Brief, unclassified description of the matter;

(7) Unique identification number;

(8) Number of copies of documents generated or reproduced; and

(9) Disposition (for example: destruction, downgrading, declassification or dispatch outside the facility, or incorporation in another accountability record) of the matter and the date.

(10) Contract or other written retention authority that authorizes the matter to be in the possession of a contractor, which should be readily available to facilitate compliance disposition reviews.

e. Inventory. An annual inventory of accountable matter shall be conducted. Each item listed in an accountability record must be visually verified and the contents of all containers authorized for storage of classified matter examined to ensure that all accountable matter has been entered into the accountability system. A report of unresolved discrepancies shall be submitted in accordance with DOE 5639.1.

f. Records Disposition. Records maintained to control and account for classified matter, including those reflecting receipt, dispatch, and destruction, shall be retained in accordance with DOE 1324.2A, and the National Archives Records Administration's General Records Schedules.

g. Working Papers and Drafts. Classified working papers and drafts are considered to be interim production stages toward the generation of a permanent document. Working papers shall be:

(1) Protected in accordance with the assigned classification;

(2) Destroyed when no longer needed; and

(3) Accounted for (if required) and controlled in the manner prescribed for a finished document of the same classification when:

(a) Released by the originator outside the activity,

(b) Retained for more than 180 days from the date of origin, or

(c) Filed permanently.

h. Automated Information System Media.

(1) Removable storage media that contains accountable classified information shall be entered into accountability in the same manner as working papers and drafts. Appropriate data regarding the existence of accountable fixed media shall be identified in the security plan and maintained with the system documentation. Accountability is not required for storage media that contains non-accountable classified information.

(2) Accountability is not required for individual files/documents contained on storage media regardless of the classification level involved. Contractors, however, must maintain a system identifying the contracting activity, the classified contract, and a general description of the TOP SECRET information contained on the storage media in the event of loss or compromise. This requirement may be accomplished through maintaining current back-up copies of the information, generating a directory listing/index of the classified files, or documenting the classified files accessed in the security operation log.

6. REPRODUCTION.

a. General.

(1) Documents may contain markings that limit reproduction without the specific, written approval of the originator.

(2) Departmental Elements and contractors shall establish local controls for the reproduction of classified documents. Reproduction of classified documents shall be limited to the minimum number of copies consistent with operational requirements and any further reproduction limitations shown on the document.

(3) Reproduced copies are subject to the same protection and control requirements as the original.

(4) Reproduction restrictions shall not restrict the reproduction of documents to facilitate review for declassification. However, after such reviews, reproduced documents remaining classified must be destroyed in accordance with page III-22, paragraph 9.

b. Top Secret. Only TOP SECRET Control Officers may reproduce TOP SECRET documents. TOP SECRET matter shall not be reproduced or photographed without written authorization. However, an approved contract which requires generation or reproduction of TOP SECRET matter will satisfy this requirement, and additional authorization will not be required.

c. Secret and Confidential. Unless specifically prohibited, SECRET and CONFIDENTIAL documents may be reproduced without the permission of the originator. Documents shall only be reproduced in the performance of official and contractual duties.

d. Equipment. Classified documents shall be reproduced on equipment specifically designated for such purpose. To the greatest extent possible these machines shall be located within Limited Areas, Protected Areas, or Exclusion Areas.

e. Mailing Lists. When graphic arts facilities receive standard mailing or distribution lists for the purpose of mailing reproduced classified documents, either the appropriate Departmental Element or the prime contractor is responsible for verifying the need-to-know, facility approval, and protection capability of the intended recipients of the documents. If this requirement and appropriate instructions have been levied on the graphic arts facility in the contract or subcontract, additional verification is not necessary. Any changes in the standard mailing list are also the responsibility of DOE or the prime contractor.

7. RECEIPT AND TRANSMISSION

a. General. Classified matter may only be transmitted in the performance of official and contractual duties. Unless the transmission is required by the specific terms of the contract or required for performance of the contract, written authorization of the contracting Departmental Element is required prior to contractors transmitting classified matter outside a facility.

b. Receiving. When classified matter is received at a facility, the following controls shall apply.

(1) Classified matter shall be delivered unopened to personnel designated to receive it at a control station(s) or TOP SECRET Control Officer. In addition, procedures shall be established to ensure that authorized personnel deliver such mail to the control station(s) with the inner container unopened, when U.S. Registered Mail, U.S. Express Mail, U.S. Certified Mail, or classified matter delivered by messenger is not received directly by the designated control station personnel.

(2) The package shall be examined for any evidence of tampering, and the classified contents checked against the receipt. Evidence of tampering shall be reported promptly to the cognizant DOE security office. If the matter was received through the U.S. Postal System, the appropriate U.S. Postal Inspector shall also be promptly notified. Discrepancies in the contents of a package shall be immediately reported to the sender. If the shipment is in order, the receipt shall be signed and returned to the sender.

c. Packaging. Classified matter to be transmitted outside a facility shall be double-wrapped (enclosed in opaque inner and outer containers) except as specified below.

(1) When envelopes are used for packaging, the classified information shall be protected from direct contact with the inner envelope by a cover sheet. The inner envelope shall be sealed and marked with the receiver's and the sender's classified mailing addresses, the highest classification of the contents and any appropriate caveats. The outer envelope shall be marked with the receiver's and the sender's classified mailing addresses. No markings or notations shall be made indicating that the contents are classified.

(2) If the item is of a size, bulk, weight, or nature precluding the use of envelopes for packaging, other containers of sufficient strength and durability shall be used to protect the item while in transit. To prevent items from breaking out and facilitate the detection of tampering, seals, puncture resistant material, wire mesh, or other knife-slash resistant material shall be used for packaging. As long as the item is enclosed in a double container, the matter may be wrapped or boxed in paper, wood, metal, or a combination thereof. The inner package shall be addressed to a classified mailing address, return addressed to a classified mailing address, and marked with the highest classification of the contents and any appropriate caveats. The outer container shall be addressed to a classified mailing address, return addressed to a classified mailing address, and sealed with no markings to indicate that the contents are classified.

(3) If the classified matter is an internal component of a packaged item of equipment with an outside shell or body which is unclassified and completely shields the classified internal component from view, the shell or body may be considered as the inner container. The shell or body shall be marked with the classification of the equipment but the address and return address may be omitted. The outer container shall be addressed to a classified mailing address, return addressed to a classified mailing address, and sealed with no markings or notations to indicate that the contents are classified.

(4) If the classified matter is an inaccessible internal component of a bulky item of equipment that can not be reasonably packaged, such as a missile, no inner container is required and the outside shell or body may be considered as the outer container, if it is unclassified. If the shell or body is classified, the matter shall be draped with an opaque covering that will conceal all classified features. The covering must be capable of being secured to prevent inadvertent exposure of the item.

(5) If specialized shipping containers, including closed cargo transporters, are used for transmitting classified matter, the container may be considered as the outer container. The address may be omitted from the inner and outer container for shipments in full truckload lots, when such an exception is contained in the provisions of the contract. Under no circumstances will the outer container, or the shipping document attached to the outer container, reflect the classification of the contents or the fact that the contents are classified.

(6) If a locked briefcase is used to hand-carry classified matter, the briefcase may serve as the outer container. The inner container shall be addressed, return addressed, and marked with the highest classification of the contents and with any appropriate caveats. The briefcase (outer container) must indicate the return classified mailing address and shall contain no markings to indicate that the contents are classified. A briefcase may not serve as the outer container when travelling aboard commercial aircraft.

d. Receipts. For all accountable and all SECRET matter, DOE F 5635.3, "Classified Document Receipt," or a receipt comparable in content, shall be used for the transmittal of classified matter outside of facilities. Receipts shall identify the classified contents and the name and address of both the sending and receiving facilities. Receipts shall not contain classified information. The receipt shall be placed inside the inner container. If not practical, the receipt may be sent to the recipient with the required advance notification of shipment or it may be hand-carried.

(1) Exceptions. With the exception of accountable matter, receipts are not required for:

(a) transmission within a facility;

(b) hand-carrying of matter; and

(c) transmittal of CONFIDENTIAL matter.

(2) Top Secret. Transmittal of TOP SECRET matter shall be controlled by a continuous receipt system, both inside and outside the facility. DOE F 1540.2, "Courier Receipt" shall be used by the TOP SECRET Control Officer when TOP SECRET matter is transmitted by a courier.

(3) Suspense Copy. A duplicate copy of receipts shall be maintained in a suspense file at the control station until the signed receipt is returned. A suspense date (normally not toexceed 30 days) shall be established, and followup action shall be initiated if the signed receipt, or similar written confirmation, is not returned within the suspense period. If the followup action is unsuccessful, an inquiry shall be conducted and the possible loss of the matter shall be reported in accordance with DOE 5639.1. Copies of signed receipts for classified matter shall be retained at control stations in accordance with DOE 1324.2A, and the National Archives and Records Administration's General Records Schedules.

e. Classified Mailing Address. Classified matter shall be addressed only to classified mailing addresses. Classified mailing addresses must be verified through the Safeguards and Security Information Management System. Office code letters, numbers, or phrases shall be used in an attention line for internal routing. When classified matter must be sent to individuals operating at a cleared facility, engaged as a consultant, or to any facility at which only one employee is assigned, the outer container shall specify:

TO BE OPENED BY ADDRESSEE ONLY
POSTMASTER -- DO NOT FORWARD
IF UNDELIVERABLE TO ADDRESSEE,
RETURN TO SENDER

Mail addressed in this manner shall be delivered only to the addressee or to an agent the addressee has authorized in writing to receive such mail. Only personnel having an appropriate access authorization may be designated as agents for the addressee.

f. Within Facilities. Classified matter transmitted within a facility shall be prepared in a manner that ensures adequate security protection for the classification involved and the method of transmission. Double-wrapping is not required; however, in all cases, measures shall be taken to protect against unauthorized disclosure. The matter may be transmitted by:

(1) Personnel having an appropriate access authorization for the level and category of classified information involved; or

(2) Approved electrical means.

g. Top Secret Outside of Facilities.

(1) Individuals may be authorized to hand-carry TOP SECRET in accordance with page III-17, paragraph 7j.

(2) When authorized by the Director of Safeguards and Security, TOP SECRET may also be transmitted by the Defense Courier Service, or Department of State Courier System.

(3) TOP SECRET may be transmitted over approved communications networks. See DOE 5300.3D, TELECOMMUNICATIONS: COMMUNICATIONS SECURITY, for secure communications requirements.

(4) Outside the U.S., provided that the means of transportation is under United States military control or under United States registry, matter may be transmitted in the custody of a cleared individual, who is authorized and specifically approved by a responsible Department of Energy authority for safeguards and security. Written authorization from Headquarters, Office of Safeguards and Security, must be obtained prior to hand-carrying TOP SECRET outside of the U.S.

h. Secret Outside of Facilities.

(1) SECRET matter may be transmitted by any method approved for the transmission of TOP SECRET matter.

(2) SECRET matter may be transmitted through the following postal services:

(a) United States Postal Service registered mail, and U.S. Postal Service Express Mail within and between the 50 States, the District of Columbia, and Puerto Rico. The Waiver of Signature and Indemnity Block of the U.S. Postal Service Express Mail label 11-B may not be executed and the use of external (street side) express mail collection boxes is prohibited.

(b) United States Postal Service registered mail through Army, Navy, or Air Force Postal Service facilities, provided that the approval of Headquarters Office of Safeguards and Security is obtained and information does not pass out of U.S.-citizen control and does not pass through a foreign postal system. This method may be used in transmitting SECRET matter to and from U.S. Government or U.S. Government contractor employees or members of the U.S. armed forces in a foreign country.

(c) Canadian registered mail with registered mail receipt in transmitting matter to and between United States Government and Canadian Government installations in the 50 States, the District of Columbia, and Canada.

(3) Commercial express service organizations may be used for the transmission of SECRET matter in accordance with the provisions contained in paragraph 7m, below.

i. Confidential Outside of Facilities.

(1) CONFIDENTIAL matter may be transmitted by any method approved for the transmission of SECRET matter.

(2) U.S. Postal Service Certified within the 50 States, the District of Columbia, Puerto Rico, and U.S. territories or possessions.

j. Authorized Hand-carriers and Escorts. Employees having an appropriate access authorization may be designated to hand-carry or escort classified matter. Hand-carrying classified matter for the purpose of a meeting or visit outside a facility shall be authorized only after a determination has been made that: (i) an unusual situation warrants such action; (ii) the classified matter is not available at the destination; (iii) the time does not permit transmission by other authorized methods; (iv) the classified matter can be properly handled and protected during transmission; and (v) the transmission can be successfully completed on the same day and the classified matter can be appropriately stored upon arrival. Only the classified matter absolutely essential for the purpose of the visit or meeting may be hand-carried by the employee.

(1) The authorized individual shall have an access authorization commensurate with the level of the information involved.

(2) The removal of classified matter from approved facilities to private residences or other unapproved places (e.g., hotel or motel rooms) is prohibited. Therefore, travelers anticipating a destination arrival time outside normal duty hours shall make prior arrangements for storage of classified matter through the host security office. All classified matter, when not in the possession of authorized individuals, shall be stored only in approved facilities.

(3) A responsible facility official shall brief a hand-carrier who does not routinely act as an authorized individual on the responsibilities to protect classified information.

(4) The authorized individual shall retain the classified matter in their possession at all times. Arrangements shall be made in advance of departure for overnight storage at an approved facility that has appropriate storage capability.

(5) When escorting shipments of classified matter via rail, individuals shall travel in an escort car accompanying the shipment, keeping the shipment car(s) under observation. When practicable and time permits, individuals shall detrain at stops to watch the shipment car(s) and check car(s) or container locks and seals. In addition, individuals shall maintain liaison with train crews, other railroad personnel, special police, and law enforcement agencies, as appropriate.

(6) When escorting shipments of classified matter via motor vehicle, individuals shall maintain continuous vigilance for the presence of conditions or situations that might threaten the security of the cargo, and take appropriate action as circumstances might require to avoid interference with the continuous safe passage of the vehicle. In addition, individuals shall check seals and locks at each stop when time permits, and observe vehicles and adjacent areas during stops or layovers.

(7) When escorting shipments of classified matter by means of commercial or military aircraft, individuals shall provide continuous observation of plane and cargo during ground stops and of cargo during loading and unloading operations.

(8) Employees authorized to hand-carry classified matter aboard commercial passenger aircraft shall follow procedures established in FAA circular 108-3 and be briefed on their overall responsibility to safeguard the classified matter and on established procedures.

k. Commercial Express Service Organizations. The use of commercial express delivery service for transmitting classified matter is restricted to emergency situations where the information positively has to be at the receiving facility(ies) on the next working day. Commercial express service shall not be used as a matter of routine or convenience for transmitting classified matter. As a minimum, the sender shall ensure that:

(1) The express service organization has been approved for the shipping and receiving locations. Approval shall be accomplished by use of DOE F 5600.2, "Facility Data and Approval Record."

(2) The transmittal address is correct and, in some instances, the appropriate, special facility handling instructions are used for such service.

(3) The intended recipient(s) is notified of the proposed shipment and arrival date.

(4) The properly wrapped package is hand-carried to the express mail dispatch center in sufficient time to allow for dispatch on the same day.

(5) Since express terminals as a matter of policy are not approved for storage of classified matter, overnight service is not used on Fridays or on the day preceding a holiday unless prior assurance has been received from the intended recipient that someone will be available at the facility(ies) to receive the shipment on arrival.

l. Common Carrier Shipments. The following classes of common carrier services may be utilized upon approval by the cognizant local safeguards and security authority, including:

(1) Motor carriers in exclusive use that provide locked and sealed van service.

(2) Locked and sealed railroad car, provided the carrier shall furnish a report on request identifying the car location.

(3) Air carriers providing prompt tracking and special signature services.

(4) Commercial messenger services engaged in the intracity/local area delivery (same day delivery only) of classified matter between cleared facilities and to the U.S. Post Office.

(5) Rail, truck, or air without escort, or special protective services, when size and weight together preclude removal without the aid of mechanical devices, and when the containers are securely banded, sealed, and otherwise fastened so as to readily reveal any attempted opening or unauthorized access.

m. Additional Requirements. Shipments of classified matter, including bulk document shipments, are subject to the following conditions, unless more stringent requirements are imposed elsewhere:

(1) Contents shall be securely packaged and shall meet applicable regulations (including those of the Department of Transportation).

(2) Seals or other positive fastening devices shall be used on shipping vehicles and containers, and be placed in a manner to show evidence of tampering. The type of seal to be used is to be determined by local safeguards and security authority. Seals shall have serial numbers. Seal identification shall be entered on bills of lading or other shipping papers. Seal numbers shall be verified by the consignee upon arrival of a shipment.

(a) General Services Administration-approved combination padlocks shall be used to secure closed cargo areas of vehicles, vans, and railroad cars.

(b) Shipments of SECRET or CONFIDENTIAL matter received at common carrier terminals shall be picked up by the consignee during the same working day, unless the carrier provides continuous protective service to the address of the consignee under locally approved procedures.

(c) Unescorted shipments by rail or truck (e.g., truckload or carload) shall be made under arrangements with carriers to provide in-transit reports as needed. The carrier shall provide immediate notice concerning any serious delay of the shipment.

(3) Assurances and Notifications.

(a) Carrier must be approved according to DOE 5634.1B.

(b) Notification of shipments shall be transmitted prior to departure either to the consignee or to the Departmental Element exercising administrative jurisdiction over the consignee, with sufficient time and information to enable proper handling at the destination. As a minimum, the notification shall include the nature of the shipment, means of shipment, number of seals, anticipated time and date of arrival, and requested notification if not received by a specified time.

(c) The consignee shall advise the consignor of any shipment not received within 48 hours after the estimated time of arrival furnished by the consignor or transshipping activities personnel. Upon receipt of such notice, the consignor shall immediately initiate tracing of the shipment.

(4) Protective Measures. Protective measures for Departmental security shipments are as follows:

(a) Appropriately authorized and cleared personnel, designated by name or title and given written authority by the responsible manager, may hand-carry, transport, or escort classified matter. Sufficient personnel shall be tasked for a specific movement assignment to ensure continuous protection of the matter being transported.

(b) Use of rail, truck, air, and other modes of transportation shall be based on protection meeting the requirements outlined in subparagraphs 1, and 2 below.

1 As a minimum, the common carrier or other service shall be required to provide the following security services:

a Surveillance by an authorized carrier employee when the classified matter is outside the vehicle.

b A tracking system that ensures prompt tracing of the shipment while en route.

c When storage is required, classified matter shall be stored in an alarmed or guarded storage area with immediate response by a carrier employee, commercial guard, or police officer.

2 Verification shall be made of the identity and authorization of person(s) who pick up the classified matter.

8. CONTRACT CLOSEOUT/FACILITY TERMINATION

a. General. Classified matter received or generated in the performance of a classified contract shall be returned to DOE on completion of the contract unless the matter has been declassified, destroyed, or retention is authorized.

b. Contract Completion. Within 120 days after completion or termination of a contract, the contractor must submit, to the Contracting Officer, either a certification of non-possession or a certification of possession. The Contracting Officer shall then transmit the certifications to the cognizant security office.

c. Certification of Non-possession.

(1) Upon return or destruction of all classified matter pertaining to a contract, the contractor shall submit a certification of non-possession. The certification must include the contract number and a statement that all classified matter has been returned or destroyed.

(2) When a Departmental Element's facility approval is to be terminated, a certificate of non-possession must be completed as part of the facility termination process.

d. Certification of Possession.

(1) Requests to retain classified shall indicate the benefit to DOE and the intended use of the information. Certifications must specifically identify each piece of TOP SECRET matter and identify SECRET and CONFIDENTIAL matter by subject matter, the type or form, and the quantity of matter.

(2) If the classified matter will aid the U.S. Government in performing another active contract and the matter is being transferred to the active contract, a copy of the retention notification shall be provided to the Departmental Element or the other Government agency holding the contract. If the contractor is not notified to the contrary, the matter may be transferred and will fall under the jurisdiction of the gaining contract.

(3) When a certification of possession is submitted, the contractor may maintain the classified matter for 2 years unless notified to the contrary by the appropriate Departmental Element.

e. Termination of Facility Approval. Notwithstanding the provisions for retention outlined above, if a facility approval is terminated for any reason, classified matter in the facility's possession shall be returned to DOE or disposed of in accordance with instructions from the Departmental Element.

9. DESTRUCTION

a. General. Departmental Elements and contractors shall establish procedures for an ongoing review of their classified holdings to reduce their classified inventory to the minimum necessary. Multiple copies, obsolete matter, and classified waste shall be destroyed as soon as practical. Classified matter shall be destroyed in accordance with records disposition schedules, including the National Archives and Records Administration General Records Schedules.

b. Methods. Classified matter shall be destroyed beyond recognition to preclude reconstruction. Destruction can be accomplished by burning, shredding, pulping, melting, mutilation, chemical decomposition, or pulverizing. Other approved methods such as disintegration, shredding, or burning shall be used to destroy paper products, as well as non-paper material such as mylar. Classified microforms may be destroyed by burning, chemical decomposition, disintegration, or other methods approved by the Departmental Element. The following additional requirements must be satisfied when classified matter is destroyed.

(1) The Departmental Element must approve public destruction facilities or any other alternative procedures (e.g., burying or disassembly).

(2) Classified matter shall be destroyed on the same day it is removed from the facility. A record of dispatch is not required unless custody of the matter is released to another contractor or a Government Agency.

(3) Ash residue produced by burning must be examined and reduced by physical disturbance to ensure that the matter is completely destroyed and no unburned matter remains.

c. Equipment. Classified matter shall be destroyed by equipment which has been approved by the cognizant security office. The residue output shall be inspected each time destruction is effected to ensure that established requirements are met.

(1) Crosscut shredders which produce residue particle size not exceeding 1/32 of an inch in width by 1/2 inch in length, may be used for destruction of classified paper and non-paper products, except microforms.

(2) Pulping equipment shall be equipped with security screens with perforations of 1/4 inch or smaller.

(3) Pulverizing equipment shall be outfitted with security screens that meet these specifications:

(a) Hammer mills - the perforations shall not exceed 3/16 inch in diameter.

(b) Choppers and hybridized disintegrators -the perforations shall not exceed 3/32 inch in diameter.

NOTE: When self-processing film or paper is used to photograph or reproduce classified information, all parts of the last exposure shall be removed from the camera and destroyed as classified waste, or the camera shall be protected at the classification level (and category if RD or FRD) of information contained on the media.

d. Witnesses.

(1) The destruction of classified matter shall be accomplished by individuals having appropriate access authorization commensurate to the classification of matter to be destroyed.

(2) The destruction of SECRET or CONFIDENTIAL may be accomplished by one individual. The destruction of TOP SECRET matter shall be witnessed by an appropriately cleared individual other than the person destroying the matter. Facilities with only one employee having the appropriate access authorization shall contact their Departmental Element's security organization for guidance on destruction.

e. Records of Destruction.

(1) Accountable Matter. Destruction of accountable classified matter must be documented by using DOE F 5635.9, "Record of Destruction", which shall be signed by the individual destroying the matter. An audit trail must be maintained until destruction.

(2) TOP SECRET. When TOP SECRET matter is destroyed, a DOE F 5635.9 shall be executed indicating the date of destruction and identifying the matter destroyed. The certificate shall be signed by the individual designated to destroy the matter and the witness to the destruction.

(3) Disposition of Records. DOE F 5635.9 must be maintained in accordance with DOE 1324.2A, and the National Archives Records Administration's General Records Schedules.

f. Waste. Classified waste shall be destroyed by approved methods as soon as practical. Receptacles utilized to accumulate classified waste shall be clearly marked to indicate its purpose. Pending destruction, classified waste and receptacles shall be protected as required for the level of classified matter involved.

CHAPTER IV

PROTECTION OF UNCLASSIFIED IRRADIATED REACTOR FUEL IN TRANSIT

1. GENERAL REQUIREMENTS FOR THE PACKAGING AND TRANSPORTATION OF IRRADIATED REACTOR FUEL. Unclassified irradiated reactor fuel shall be packaged and transported in accordance with DOE 1540.1A,MATERIALS TRANSPORTATION AND TRAFFIC MANAGEMENT, DOE 1540.2, HAZARDOUS MATERIAL PACKAGING FOR TRANSPORT - ADMINISTRATIVE PROCEDURES, and DOE 5480.3, SAFETY REQUIREMENTS FOR THE PACKAGING AND TRANSPORTATION OF HAZARDOUS MATERIALS, HAZARDOUS SUBSTANCES, AND HAZARDOUS WASTES. Advance written notification on shipments shall be made to Governors of States, or their designees, and Tribal officials, through which any shipments shall pass according to DOE 1540.1A, page II-13, paragraph 8.

2. GENERAL REQUIREMENTS FOR PHYSICAL PROTECTION OF IRRADIATED REACTOR FUEL IN TRANSIT. A physical protection system shall be established and maintained to include:

   a. All shipments of DOE unclassified irradiated reactor fuel will utilize the DOE Transportation Tracking and Communications System (TRANSCOM) for communications between the transport vehicle, TRANSCOM control center, and the responsible field element/contractor Emergency Operations Center.

   b. A carrier's communications center at a designated location which will be staffed continuously by at least one individual who will monitor the progress of the irradiated reactor fuel shipment and will notify DOE and other appropriate agencies if an emergency should arise.

   c. Carrier emergency response procedures which are to be implemented as required.

   d. A written log by the shipper and receiver for each irradiated reactor fuel shipment that will include information describing the shipment and significant events that occurred and are reported or recorded by the escort during the shipment and conditions/inventory of the shipment received. Any significant events or unusual circumstances involved in receipt of the shipment should be included. These logs are to be available for review by authorized DOE personnel and shall be maintained in accordance with the DOE Records Management Program.

   e. The route plan shall contain a statement of origin and destination points, a route selected in compliance with this section, all planned stops, estimated departure and arrival times.

f. Highway transport vehicles equipped with consignor-approved feature(s) for immobilization of the tractor or cargo-carrying portion of the transport vehicle for at least 30 minutes or a method to enhance the ability of a communications center or response force to locate the transport vehicle's position if an incident occurs, e.g., the TRANSCOM.

g. The transport vehicle driver is familiar with, and is capable of, implementing transport vehicle immobilization, communications, and other security procedures.

h. Railroad routing shall give consideration to the class of railroad, class of track, reducing time in transit, time at interchange points, number of carriers, and cost of service. It may be necessary to consult with, and receive recommendations from, the Federal Railroad Administration and/or the railroads concerning data for route selection.

i. Shipment planning to assure scheduled intermediate stops are minimized to the extent practicable.

j. At least one escort with appropriate communication equipment to maintain visual surveillance of the shipment during periods when the transport vehicle is stopped or the shipment vessel is docked.

k. Shipping papers which conform to Department of Transportation regulations and contain the telephone number of the DOE communications center having jurisdiction, with instructions to report (1) status of the shipment periodically, and (2) emergency situations at any time.

l. Carrier instructions which provide that escorts make periodic calls to the communications center to advise of the status of the shipment for road and rail shipments and for sea shipments while shipment vessels are docked at U.S. ports.

m. The Department may, at its option, assign a health physicist or another professional to accompany rail shipments to advise or assist the escort in an emergency, as requested. These employees may be required to execute a hold-harmless agreement per Rule 43 of the Uniform Freight Classification.

3. SPECIFIC REQUIREMENTS FOR PHYSICAL PROTECTION OF IRRADIATED REACTOR FUEL IN TRANSIT.

a. Requirements for the Physical Protection of Shipments of Unclassified Irradiated Reactor Fuel Cooled 150 Days or More.

(1) Escort Communications. Shipment escorts shall maintain continuous communication capability with a communications center through use of TRANSCOM as the primary means of communication. In the event of problems with TRANSCOM, telephonic contact at 2 hour intervals will be employed to advise of the status of the shipment for

road and rail shipments and for sea shipments while shipment vessels are docked at U.S. ports.

(2) Shipments by Highway. In addition to the general provisions of this Order, the physical protection system for an unclassified irradiated reactor fuel shipment by highway shall assure:

(a) The transport vehicle, while in motion, is occupied by at least two drivers who alternate as vehicle operator and escort.

(b) Escort has the capability of communicating with the carrier's communications center and/or another designated communications center, and local law enforcement agencies, through the use of:

1 Citizens band radio; and

2 Mobile telephone or other equivalent means of communication.

(c) Both drivers shall possess the required Department of Transportation training credentials.

(d) Stops for food, fuel, rest, and phone calls are to be coordinated to minimize their number per trip and duration. When stopped, the vehicle must be attended or kept under visual surveillance by the escort or driver to impede simple cases of unauthorized access, otherwise assistance is to be summoned.

(3) Shipments by Rail. In addition to the general provisions of this Order, the physical protection system for an irradiated reactor fuel shipment by rail shall assure:

(a) A railroad employee shall be assigned the duties of an escort. This employee will be stationed at a location on the train that will permit observation of the shipment car while in motion.

(b) The escort, through the conductor, has the capability of communicating with the railroad communications center and local law enforcement agencies through the use of an on-board radiotelephone or other equivalent means of communication, which must be available on the train.

(c) When the train is stopped en route on the mainline or on a siding, escorts will follow standard emergency response procedures of the railroad designed to deter trespassers, to protect railroad property, and to provide physical protection of the shipment for which the railroad is responsible as a bailee. Instructions or assistance will be requested from the communications center as required. Arrangements for such assistance should be planned and coordinated sufficiently in advance of a shipment so as to assure maximum protection levels from this resource.

(d) When a shipment car is stopped in a railroad yard awaiting classification and/or interchange, the responsibility for visual surveillance passes to special agents and/or yard watchmen responsible for yard security and can provide physical protection of the shipment car.

(4) Shipments by Sea. In addition to the general provisions of this Order, the physical protection system for any portion of an irradiated reactor fuel shipment that is by sea shall assure:

(a) While within U.S. territorial waters or while docked at a U.S. port, the ship's duty officer will assure the shipment is unloaded only as authorized by the consignees.

(b) Ship's officers, when in U.S. territory, have the capability of communicating with port authority police and/or Coast Guard communications centers through the use of radiotelephone or other equivalent means of communications to summon assistance as required.

(c) Public access to the cargo dock areas and berthed vessels is restricted by fencing and/or uniformed port authority police who are armed.

(d) While at sea or in a foreign port, the master of the vessel will provide physical protection according to the terms of the ocean bill of lading or the charter and according to international conventions.

b. Requirements for the Physical Protection of Irradiated Reactor Fuel Cooled for Less Than 150 Days. When the Department ships fuel which has been cooled for less than 150 days, the provisions of 10 CFR 73.37 shall apply. However, this requirement does not apply to reactor fuel specimens which, as a matter of technical necessity, need to be transported between research facilities within 150 days after being removed from a test facility which is not part of a power generation or production reactor. For such specimens, the provisions of this Manual for Category IV quantities of SNM (highly irradiated forms) shall apply regardless of the cooling period, unless higher levels of protection are dictated by the attractiveness of the material as a radiological sabotage target.

4. INSTRUCTIONS AND TRAINING REQUIREMENTS FOR ESCORTS. Escorts, truck drives, train crews, and ship's officers responsible for shipments of unclassified irradiated reactor fuel via commercial carriers shall be specifically trained in appropriate requirements prior to being authorized to perform such duties.

CHAPTER V

SECURITY AND RESTRICTED ACCESS AREAS

1. GENERAL. See paragraph 2, page V-3, for Property Protection Area requirements. The following requirements apply to Security Areas, except Property Protection Areas:

   a. Access shall be controlled to limit entry to appropriately cleared and/or authorized individuals.

      (1) Any person allowed to enter a Security Area who does not possess an access authorization at the appropriate level will be escorted at all times by a cleared and knowledgeable individual.

      (2) Local authorities shall establish escort-to-visitor ratios in a graded manner for each of these Security Areas. Escort requirements for Property Protection Areas shall be determined by local authorization.

   b. Controls shall be established to detect, assess, deter, and (in certain cases) prevent unauthorized access to Security Areas.

   c. Access control requirements may be layered as appropriate for the situation. At succeeding boundaries, access controls may be increased.

   d. A personnel identification system (e.g. security badge system) shall be used to control access into Security Areas.

   e. Automated access control systems may be used as approved by the cognizant local Departmental authority for safeguards and security.

   f. Means shall be provided 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. The protection program shall include suitable means to assess alarms. See paragraph 1, page VI-1 for amplified requirements.

   g. Entrance/exit inspections, as required, shall be made by protective personnel or with detection equipment designed to detect prohibited articles (See subparagraph (2), below). Inspections of personnel, hand-carried items, and/or vehicles shall provide reasonable assurance that prohibited articles are not introduced and that safeguards and security interests are not removed from the area without authorization.

      (1) Inspections. Inspection procedures, requirements, and frequencies shall be developed based on a graded approach and included in the appropriate security plan. Where random entry or exit inspections are permissible, the inspection shall be conducted on

a percentage basis, determined by the Departmental cognizant local authority for safeguards and security, using techniques that ensure randomness.

(2) Prohibited Articles. The following articles are prohibited from Security Areas, unless approved by the cognizant Departmental local authority for safeguards and security: any dangerous weapon, explosive, or other dangerous instrument or material likely to produce substantial injury or damage to persons or property. (Reference Title 10 CFR Part 860, and Title 41 CFR Part 101-19.3.) Sites shall, at a minimum, employ administrative procedures to deter the introduction of explosives into Security Areas.

(3) Security Area Controlled Articles. The following privately owned articles are not permitted in a Limited Area, Exclusion Area, Protected Area, or Material Access Area without prior authorization.

(a) Recording equipment (audio, video, optical, or data).

(b) Electronic equipment with a data exchange port capable of being connected to automated information system equipment.

(c) Cellular telephones.

(d) Radio frequency transmitting equipment.

(e) Computers and associated media.

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

(g) Other items prohibited by law.

(4) Concentric Security Areas. When a Security Area, excepting Material Access Areas, is within a larger Security Area, additional entry/exit inspections are not required at the inner Security Area perimeter if inspections conducted at the outer Security Area boundary are at the same level as required for the inner Security Area boundary. Entry and exit inspections shall be conducted at Material Access Area boundaries regardless of outer boundary inspections.

h. Clearly defined physical barriers, such as fences, walls, and doors, shall be used to define the boundary of a Security Area. Barriers shall meet the following requirements, as well as supplementary requirements at paragraph 1, page VII-1:

(1) Barriers shall direct the flow of personnel and vehicles through designated entry control portals.

(2) Barriers and entry control portals, supplemented by other systems such as patrols or surveillance, shall be used to deter and detect introduction of prohibited articles or removal of safeguards and security interests.

(3) 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.

(4) Barriers shall be capable of controlling, impeding, or denying access to a Security Area.

i. Signs reflecting information on: the Atomic Weapons and Special Nuclear Rewards Act; prohibited articles; the inspection of vehicles, packages, or persons either entering or exiting; notification of video surveillance equipment; and trespassing, if applicable, shall be posted. Signs prohibiting trespassing shall be posted around the perimeter and at each entrance to a Security Area except when one Security Area is located within a larger posted Security Area. See Chapter XIII for further details.

j. Visitor logs are required at Protected Areas, Material Access Areas, and Exclusion Areas. Requirements for other Security Areas, if any, and procedures for visitor logs at Security Areas shall be developed and approved by the cognizant local Departmental authority for safeguards and security. DOE F 1240.1, "Foreign Visitors Security Register," and DOE F 5630.6, "Visitors Security Register," shall be used. Logs shall be retained in accordance with DOE 1324.2A, RECORDS DISPOSITION and General Records Schedule 18.

2. PROPERTY PROTECTION AREA. A Property Protection Area is 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 systems, protective personnel, intrusion detection systems, and locks and keys. Protective measures taken shall provide appropriate, graded protection.

a. Access controls, where determined to be necessary by local authority, shall be implemented to protect Departmental property and facilities.

b. Signs prohibiting trespassing, where necessary, shall be posted around the perimeter and at each entrance to the Property Protection Area in accordance with Title 10 CFR Part 860, "Trespassing on Administration Property" and Title 41 CFR Part 101-19.3, "Federal Property Management Regulation." See Chapter XIII.

c. Vehicles and hand-carried items entering or leaving shall be subject to inspection to deter and detect unauthorized removal of Government assets.

d. Physical barriers, where determined to be necessary by local authority, shall be used to protect property and facilities.

3. LIMITED AREA. A Limited Area is 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.

   a. Requirements. A Limited Area shall have barriers identifying its boundaries and encompassing the designated space, as well as access controls to provide reasonable assurance that only authorized personnel are allowed to enter and exit the area. Limited Area access requirements shall be administered as follows:

      (1) Individuals permitted unescorted access shall have access authorization and need-to-know consistent with the matter under protection in the area.

      (2) When access to a Limited Area is authorized for a person without appropriate access authorization or need-to-know, measures shall be taken to prevent compromise of classified matter.

      (3) Access to safeguards and security interests within a Limited Area, when not in approved storage, shall be controlled by the custodian(s) or authorized user(s).

   b. Personnel and Vehicle Access Control. 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 and shall be accomplished at the Limited Area entrance(s).

4. EXCLUSION AREA. An Exclusion Area is 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.

   a. Requirements. An Exclusion Area shall have barriers identifying its boundaries and encompassing the designated space, as well as access controls to provide reasonable assurance that only authorized personnel are allowed to enter and exit the area. Exclusion Area requirements shall be administered as follows:

      (1) An Exclusion Area shall meet all requirements for a Limited Area.

      (2) Access requirements are as follows:

         (a) Individuals allowed unescorted access shall have an access authorization and need-to-know consistent with the matter to which they would have access by mere virtue of their presence in the area.

         (b) When access to an Exclusion Area is authorized for a person without appropriate access authorization and need-to-know, measures shall be taken to prevent compromise of classified matter while the individual is in the area.

b. Personnel and Vehicle Access Control. 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.

(1) Private vehicles shall be prohibited from an Exclusion Area.

(2) 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 and authorized drivers, or those under escort by properly cleared, authorized personnel.

5. PROTECTED AREA. A Protected Area is 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. Additional requirements are as follows:

a. Inspections. Inspections for a Protected Area shall be as follows:

(1) Entrance inspections of personnel, vehicles, and hand-carried items shall be conducted to deter and detect the unauthorized introduction of prohibited articles. Specific inspection procedures and special nuclear material/metal detection levels and limitations shall be established and documented.

(2) Exit inspections of personnel, vehicles, and hand-carried items shall be conducted to deter and detect the unauthorized removal of special nuclear material. Specific inspection procedures and special nuclear material/metal detection levels and limitations shall be established and documented. When the Protected Area encompasses a Material Access Area, the exit inspections at the Protected Area boundary may be performed on a random basis with the extent and frequency determined by the cognizant local DOE authority for safeguards and security.

(a) A physical or electronic search shall be separately conducted of vehicles, personnel, packages, and all other containers at all routine exit points for Protected Areas that contain Category I quantities (or lessor quantities with credible rollup to a Category I quantity).

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

(c) Exit inspections shall be capable of detecting shielded special nuclear material (e.g., using a combination of special nuclear material and metal detectors) and

shall meet requirements for metal and special nuclear material determined by the Manager, Operations Office.

(d) Procedures used shall assure that unalarmed portals without the means to detect special nuclear material are not used.

(3) Exits shall be alarmed or controlled at all times.

(4) Protective force response time to an intrusion detection shall be less than the delay time that can be demonstrated from alarm activation until intruders could complete adverse actions.

b. Personnel and Vehicle Access Control. Validation of the identity and access authorization of persons authorized access shall be administered by armed protective force personnel and/or an automated access control system as determined by local safeguards and security authorities. Access control requirements shall be as follows:

(1) Private vehicles shall be prohibited from a Protected Area.

(2) 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. Service and delivery vehicles shall be admitted only when on authorized business and when driven or when escorted by properly cleared, authorized personnel. Entry of service and delivery vehicles shall be kept to an operational minimum.

6. VITAL AREA. A Vital Area is 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.

a. Requirements. In addition to protection strategies at a Protected Area, the following requirements shall be met:

(1) Area boundaries shall conform to the layered protection concept, with a separate Vital Area perimeter located within a separate and distinct Protected Area.

(2) The perimeter of each Vital Area shall be monitored to deter and detect unauthorized entry attempts.

(3) Vital Equipment shall be protected with an intrusion detection system.

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

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

b. Personnel and Vehicle Access Control.

(1) Validation of the identity and access authorization of persons authorized access shall be administered by protective personnel or an automated access control system as determined by local safeguards and security authorities.

(2) Private vehicles shall be prohibited from a Vital Area. 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 and authorized personnel. Service and delivery vehicles shall be admitted only when on authorized business and when driven or escorted properly cleared and authorized personnel.

7. MATERIAL ACCESS AREA. A Material Access Area is 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 a 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 perimeter located within a separate and distinct Protected Area. Material Access Area barriers shall direct the flow of personnel and vehicles through designated portals.

a. Requirements. Inspections shall provide reasonable assurance against the unauthorized introduction of prohibited articles or removal of special nuclear material by force, stealth, or deceit.

(1) Entrance inspections of personnel, vehicles, and hand-carried items shall be conducted to deter and detect the unauthorized introduction of prohibited articles.

(2) Exit inspections of personnel, vehicles, and hand-carried items shall be conducted to deter and detect the unauthorized removal of special nuclear material. Specific inspection procedures and special nuclear material/metal detection levels and limitations shall be established and documented.

(a) A physical or electronic search shall be separately conducted of vehicles, personnel, packages, and all other containers at all routine exit points for Material Access Areas that contain Category I quantities (or lessor quantities with credible rollup to a Category I quantity).

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

(c) Exit inspections shall be capable of detecting shielded special nuclear material (e.g., using a combination of special nuclear material and metal detectors) and shall meet requirements for metal and special nuclear material determined by the Manager, Operations Office.

(d) Procedures used shall assure that unalarmed portals without the means to detect special nuclear material are not used.

(3) Protective force response time to an intrusion detection shall be less than the delay time that can be demonstrated from alarm activation until intruders could complete adverse actions.

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

b. Personnel and Vehicle Access Control. Access control shall be administered by armed protective force personnel and/or automated access control systems as determined by local safeguard and security authorities.

(1) Validation of the identity, access authorization, and authority to enter for persons allowed access shall be accomplished at Material Access Area entrances.

(2) Private vehicles shall be excluded from a Material Access Area. Government-owned or Government-leased vehicles shall be admitted to Material Access Areas 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.

(3) Exit detection levels for special nuclear material and shielding shall be established consistent with the form, quantity, attractiveness level, and credible diversion amounts/attempts of special nuclear material contained within the area.

8. RESTRICTED ACCESS AREAS. Restricted Access Areas shall be administered as follows and as outlined in pertinent Departmental directives:

a. Sensitive Compartmented Information Facilities. The Department of Energy follows requirements in Director of Central Intelligence Directive 1/21 for the construction of Sensitive Compartmented Information Facilities. These facilities shall be located within Exclusion Areas.

b. Central Alarm Station. A Central Alarm Station shall be used in protection of Category I and Category II quantities of special nuclear material. A Central Alarm Station shall meet the requirements of a hardened post and shall be located, as a minimum, within a Limited Area. Requirements are as follows:

(1) An access control system shall be used to restrict admittance to persons who require access in the performance of official duties.

(2) A Central Alarm Station shall be attended constantly by personnel who possess access authorizations that are commensurate with the most sensitive asset that is under the protection of the Central Alarm Station.

(3) A Central Alarm Station protecting classified matter shall be of sound construction meeting local building codes.

c. Secondary Alarm Stations. Facilities with Category I or II quantities of special nuclear material shall have a Secondary Alarm Station. Used as an alternative alarm annunciation point to the Central Alarm Station, the Secondary Alarm Station shall be maintained at a location continuously manned, such that a response can be initiated in the event a Central Alarm Station is unable to perform its intended function. Secondary Alarm Stations shall meet the operational requirements of Central Alarm Stations with the exception of hardening and location within a Limited Area. The Secondary Alarm Station need not be fully redundant to the Central Alarm Station, but shall be capable of providing effective control response to safeguards and security incidents.

d. Local Law Enforcement Agency or Private Alarm Station. If response by local law enforcement agency/protective personnel to alarm activity is requred for facility approval, the response shall meet the specifications for Grade AA as contained in Underwriters Laboratories Standard 611, "Central-Station Burglar-Alarm Systems."

e. Secure Communications Centers and Automated Information System Centers.

(1) Centers handling classified messages or information shall be located, as a minimum, within a Limited Area.

(2) Separate access controls and barriers shall be established to restrict admittance to persons employed therein or who require access in the performance of official duties.

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

CHAPTER VI

PROTECTION ELEMENT: INTRUSION DETECTION AND ASSESSMENT SYSTEMS

1. GENERAL. Intrusion detection systems shall be installed to provide reasonable assurance that breaches of security boundaries are detected and that assessment information is provided to protective personnel. Intrusion detection systems shall be provided for Protected Areas as required at page V-5, paragraph 5, Vital Areas as required at page V-6, paragraph 6, and for Material Access Areas and special nuclear material as discussed in paragraphs 2b, 3, and 4 below. Intrusion detection systems shall be provided for protection of classified matter as described at page III-1, paragraph 3. Intrusion detection systems shall also be provided for vaults, vault-type rooms, Sensitive Compartmented Information Facilities, Classified Automated Information System facilities, and Secure Communications Centers. For other applications, the impact of loss or destruction of property and facilities shall be considered when assessing the need for intrusion detection systems.

   a. A means for timely detection of intrusion shall be provided by the use of intrusion detection systems and/or protective force fixed posts and/or mobile patrols. Timely assessment of intrusion detection system alarms shall be provided by electronic systems and/or patrols. When used for detection, patrols shall be conducted at random intervals, at a documented frequency.

   b. Intrusion detection systems shall provide operable coverage in all common environmental conditions and under all common types of lighting conditions.

   c. Visual observations by protective personnel on patrol or in fixed posts may complement intrusion detection systems and increase the probability of early detection.

   d. There shall be an effective method by which to assess intrusion detection system alarms (e.g., intrusion, false, nuisance, and tamper).

   e. Response capability to intrusion detection system alarms shall be provided to protect Departmental safeguards and security interests. The response capability may be provided by assigned protective personnel or by the local law enforcement agency, as applicable. Response times shall be appropriate for the protection strategy employed at the site.

2. REQUIREMENTS. Specifications for intrusion detection systems shall be as follows:

   a. Intrusion detection systems shall:

      (1) Employ protection in-depth with multiple detection layers for Category I and II special nuclear material targets. Complementary sensor selection is required for multilayered Protected Area perimeter applications.

      (2) Be monitored continuously by assigned personnel to assess alarms and intrusion activities and initiate appropriate responses.

(3) Be operated and maintained in a manner ensuring that the number of false and nuisance alarms does not reduce the system credibility.

(4) Be tamper-resistant or tamper-alarmed, and have components such as sensors, multiplexers, power supply cabinets, sensor processors, junction boxes, and alarm access panels that are also tamper-resistant or tamper-alarmed for intrusion detection systems protecting Protected Areas, Material Access Areas, or Vital Areas.

b. If intrusion detection alarms are not monitored by an alarm station, an audible and optional visual alarm signal capable of alerting protective personnel on patrol in the area and directing them to the location of the alarm shall be provided. The audible alarm shall be distinguishable from other types of alarms and shall be no less than 65 decibels above ambient background noise level at the farthest location of the responding protective force post.

c. Compensatory measures shall be provided during times when the intrusion detection system is not in operation or at temporary locations where a permanent intrusion detection system is not practical or cost effective.

d. Systems installed after the effective date of this Manual, used in the protection of Category I quantities of special nuclear material, shall employ redundant, independently routed communication paths to avoid a single point failure. Several intrusion detection sensors may be connected to a common data collection point. The redundant pathways shall begin at a data collection point and be conveyed and reported independently to a physically separated Central Alarm Station and Secondary Alarm Station.

e. Records shall be kept on each actual and/or false nuisance alarm. The record shall be reviewed, analysis performed, and corrective measures taken to correct system malfunctions. The record shall contain, as a minimum: date and time of the alarm; cause of the alarm or a probable cause if definite cause cannot be established; and the identity of the recorder or the operator on duty.

f. Alarm monitoring systems shall be self-checking and shall annunciate system failure in the alarm station(s). For the protection of Category I and II quantities of special nuclear material, alarms shall be annunciated in both the Central Alarm Station and Secondary Alarm Station. Systems shall indicate the type and location of the alarm source.

g. In existing intrusion detection systems, where dedicated telephone cable pairs are used to connect the intrusion detection system to the alarm station and/or annunciating point, cable pairs shall not be routed through telephone switching equipment.

h. Each sensor protected zone shall have a unique electronic address code.

3. INTERIOR SYSTEM SPECIFICATIONS. Intrusion detection systems, used to protect Secret and/or Confidential matter, Category III and IV quantities of special nuclear material, and Property Protection Areas, shall be approved by the cognizant local authority for

safeguards and security and be documented in the site security plan. Requirements for Top Secret matter, Categories I and II quantities of special nuclear material(s), and Vital Equipment are as follows:

a. Devices and equipment purchased after the date of this Manual for interior intrusion detection applications shall meet Federal Specification W-A-450-C, "Components for Interior Alarm Systems."

b. Balanced magnetic switches shall initiate an alarm upon attempted substitution of an external magnetic field when the switch is in the normally secured position.

c. A balanced magnetic switch shall initiate an alarm whenever the leading edge of the door is moved 1 inch (2.5 centimeters) or more from the door jam.

d. Volumetric detectors shall detect an individual moving at a rate of 1 foot per second, or faster, within the total field-of-view of the sensor and its plane of detection.

e. Interior intrusion detection sensors shall have less than 1 false alarm per 2,400 hours of operation per sensor. The system shall be maintained in such a way to provide reasonable assurance that the number of false and nuisance alarms does not reduce system credibility. If the alarms can be assessed at all times, either visually or by closed-circuit television, a higher false alarm rate and nuisance alarm rate may be tolerated if it does not result in system degradation. This information shall be documented.

f. Systems shall be functionally tested in accordance with established procedures at a frequency that is documented.

4. EXTERIOR SYSTEM SPECIFICATIONS. Requirements for Protected Areas, Material Access Areas, and Vital Areas are as follows:

a. The false alarm rate for the total perimeter intrusion detection system shall not average more than 1 false alarm per week, per sensor, while maintaining proper detection sensitivity. If the segments can be fully assessed at all times, either visually or by closed-circuit television, a higher false alarm rate and nuisance alarm rate may be tolerated if it does not result in system degradation. This information shall be documented.

b. The perimeter intrusion detection system shall be capable of detecting an individual (weighing 35 kilograms or more) crossing the detection zone walking, crawling, jumping, running, or rolling (at speeds between 0.15 and 5 meters per second), or climbing the fence, if applicable, at any point in the detection zone with a detection probability of 90 percent, at a 95 percent confidence level. Testing shall be conducted at the time of initial perimeter intrusion detection system installation and at least annually thereafter to validate this detection probability and confidence level. If more frequent operational testing or acceptance and validation testing indicates degradation, intrusion detection for

the problem area shall be revalidated. When calculating detection probability for multiple sensor systems, detection is assumed if any of the sensors detect the intrusion.

c. Intrusion detection systems shall cover the entire length of the perimeter of a detection area, including the tops of buildings that are situated in the detection area.

d. Unattended gates and/or portals, and where appropriate, culverts and sewers that have openings greater than 96 square inches (619 square centimeters) where the smallest dimension is greater than 6 inches (15 centimeters), shall have detection capabilities at least as effective as the rest of the intrusion detection system, except when protected by access delay systems providing delay comparable to tunnelling or wall penetration. The intrusion detection system shall be operational when the opening is not attended.

e. Intrusion detection systems in adjacent detection zones shall overlap sufficiently to eliminate areas of no detection between detection zones. The length of alarm zones shall be consistent with the characteristics of the sensors used in that zone.

f. Perimeter intrusion detection systems shall be designed, installed, and maintained in such a manner as to deny adversaries a means to circumvent the detection system.

g. The isolation zone between fences shall be at least 20 feet (6 meters) wide.

h. The isolation zone between fences shall be clear of fabricated or natural objects that would interfere with detection equipment or the effectiveness of the assessment.

i. Wires, piping, or similar objects that could be used to assist an intruder traversing the isolation zone or could assist in the undetected ingress or egress of an adversary or matter, shall be protected by the detection and assessment system or constructed in a manner that deters their use.

j. The detection zone of each intrusion detection system sensor (where applicable) shall not provide a pathway (e.g., dips, obstructions) for an individual to avoid detection.

k. The detection zone of each intrusion detection system shall be kept free of snow, ice, grass, weeds, debris, and any other item that degrades intrusion detection system effectiveness. When the above action cannot be accomplished in a timely manner, and when degradation of detection capabilities exists, compensatory measures shall be taken to provide timely detection.

l. Intrusion detection systems shall be functionally tested in accordance with established procedures at a frequency that is documented.

5. INTRUSION DETECTION SYSTEM ALARM ANNUNCIATION AT THE CENTRAL AND SECONDARY ALARM STATION.

   a. A facility possessing classified matter under the exclusive protection of a Central Alarm Station shall have its sensors connected by direct, continuously supervised, leased line, or by such other means as to distinguish its alarms from all other alarms monitored by the Central Alarm Station.

   b. Alarms shall annunciate audibly and visually to both the Central Alarm Station and the Secondary Alarm Station.

   c. Acknowledgement of alarms shall be straightforward and easily performed.

   d. Intrusion detection system status indicators shall be provided to indicate when the system is not in working order and to indicate when tampering with any major system component has occurred.

   e. Where applicable, the alarm control system shall have the capability to call the Central Alarm Station and Secondary Alarm Station operators' attention to an alarm-associated video recorder/monitor. The picture quality shall allow the operator to recognize and discriminate between human and animal presence in the camera field-of-view.

   f. Video recorders, when used, shall be actuated by alarm signals and operate automatically. The response shall be sufficiently rapid to record an actual intrusion.

   g. When used as the principal means of alarm assessment and to determine response level, closed-circuit television cameras shall have tamper-protection and loss-of-video alarm annunciation.

   h. If remote assessment of a perimeter intrusion detection system is used, the coverage shall be complete, with no gaps between zones and no areas that cannot be assessed because of shadows or objects blocking the camera field. When such conditions exist on a temporary basis, compensatory measures shall be put into effect.

6. LIGHTING REQUIREMENTS. Protective illumination shall be provided topermit detection and assessment of adversaries and to reveal unauthorized persons.

   a. Protective lighting in Protected Areas, Material Access Areas, and Vital Areas shall be adequate to provide 24-hour visual assessment.

      (1) Lights shall provide a minimum 2 foot-candle illumination at ground level for at least a 30-foot (9.14-meters) diameter around protective personnel posts, and 0.2 foot-candle illumination for 150 feet (45.72-meters) in all directions.

      (2) Where protective lighting at remote locations is not feasible, protective personnel patrols and or fixed posts may be equipped with night vision devices. Night vision

devices shall not be used routinely in lieu of protective lighting at ingress and egress points, but may be used in the event of loss of lighting.

(3) Light glare shall be kept to a minimum in situations where it would impede effective operations of protective personnel; interfere with rail, highway, or navigable water traffic; or be objectionable to occupants of adjacent properties.

(4) Light sources on protected perimeters shall be located so thatillumination is directed outward, wherever possible.

b. Protective lighting for other applications shall be as specified in local security plans.

7. AUXILIARY POWER SOURCES. Intrusion detection systems for protection of Categories I and II special nuclear material, Vital Equipment, and Top Secret matter shall have auxiliary power sources as specified below. Auxiliary power for systems protecting other assets shall be as approved in applicable security plans.

a. Auxiliary power shall be available and shall be capable of maintaining full operation of the intrusion detection and assessment system for 8 hours, or such a time as would be needed to implement contingency plans. The period of time necessary to implement contingency plans shall be documented.

b. Transfer to auxiliary power shall be automatic upon failure of the primary source and shall have no effect on operation of the security system or device. The alarm station shall receive an alarm indicating failure of the security system power and transfer to the auxiliary power source. For the protection of Category I and II quantities of special nuclear material and Vital Equipment, both the Central Alarm Station and Secondary Alarm Station shall receive the alarm.

c. Rechargeable batteries, when used, shall be kept fully charged or subject to automatic recharging whenever the voltage drops to a level specified by the battery manufacturer. Non-rechargeable batteries shall be replaced whenever their voltage drops 20 percent below the rated voltage or manufacturer's recommendations. An alarm signal shall be activated to indicate this condition.

d. Auxiliary power sources shall have the capability to facilitate operational testing or routine maintenance.

8. PROTECTION OF INTRUSION DETECTION SYSTEMS.

a. General. Security related equipment shall be protected from unauthorized access in a graded manner consistent with its importance. For protection of Categories I and II special nuclear material, Vital Equipment, and Top Secret and Secret classified matter, all detection/alarm devices, including transmission lines to annunciators, shall be tamper-indicating in both the access and secure modes. System components used for

protection of other interests shall be protected, consistent with a cost/benefit analysis determined by each facility.

b. Physical Protection. The requirements for physically protecting intrusion detection system components are listed below:

(1) See Table VI-1 for information on the location of alarm communications lines, line supervision, and testing, depending on the asset being protected.

(2) Electronics enclosures and junction boxes shall be welded shut, be under lock and key control, have tamper switches, or have tamper-resistant hardware.

c. Line Supervision. Line supervision is required for the protection of intrusion detection systems protecting safeguards and security interests, in accordance with Table VI-1. For property, line supervision may be provided consistent with a cost/benefit analysis determined by each facility. Where data encryption is used, key changes shall be made at the specified interval for manual testing. The requirements for line supervision are listed below:

(1) Classes of Line Supervision. Performance-based definitions are characterized in Table VI-2 (extracted from Federal Specification W-A-450C), with examples of each class. For consistency in Departmental applications, the following interpretations shall be used:

(a) Classes A through C shall apply to transmission of bytes of data. In general, Classes A through C apply to alarm links between data gathering panels, between data gathering panels and central alarm computers or alarm annunciator panels, and between computers.

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

(2) Line Supervision Options. Testing shall provide assurance that the line or data link is capable of transmitting an alarm signal and that it has not been compromised. Different combinations of line supervision and testing are allowed depending on link routing. The three cases of an alarm link remaining within the Security Area, going through a lower Security Area, and going through an unsecured area, are presented in Table VI-1 for the two primary segments of alarm data transmission: from sensor to data gathering panel, and from data gathering panel to data gathering panel or central processing unit.

d. Alarm Annunciation and Response. Line supervision/tamper alarms shall be annunciated in both the Central Alarm Station and Secondary Alarm Station, indicating the type of alarm and the affected equipment. For protective personnel response, a line supervision/tamper alarm shall be treated the same as an intrusion alarm for the area being protected.

TABLE VI-1. ALARM LINE SUPERVISION OPTIONS

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

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

TABLE VI-2. LINE SUPERVISION CHARACTERISTICS

CLASS	CHARACTERISTICS	EXAMPLES
A	Compromise would require the application of national lever computer analysis before the attempt to attack. A collection of encrypted data from the communication lines to be compromised shall be available for the analysis. Special equipment or software, and professional engineering skills and experience are necessary.	Digital Encryption Standard Encryption or National Security Agency-approved encryption techniques. Feedback shall be used to provide variation of the contents of the data packet in repeated transmissions of the same information.
B	Compromise would require the use of a microprocessor and prior computer analysis. The compromise will require significant competence of the technical personnel and working samples of the equipment.	Pseudo-random polling or proprietary data encryption. Where encryption is used, feedback shall be used to provide for variation of the contents of the data packet in repeated transmissions of the same information. Fiber optics cable with an optical supervision signal.
C	Compromise would require the use of special logic circuitry, without requiring the use of prior computer analysis.	Digital data packets, polling, exception reporting with polling for health checks.
D	Compromise would require the use of active analog circuitry including transistors and tape recorders.	Frequency Shift Keying of complex signal.
E	Compromise would require the application of a combination of passive or active components such as filters and phase shifters.	DC or AC line supervision.
F	Compromise would require only the insertion of a single passive of active component.	Exception reporting without polling for health checks.

CHAPTER VII

PROTECTION ELEMENT: ACCESS CONTROL AND ENTRY/EXIT INSPECTIONS

1. GENERAL.

   a. Requirements. Access control points shall meet the following requirements:

      (1) Access control points shall be designed to provide positive control over vehicular and pedestrian traffic.

      (2) Motorized gate controls, where used, shall be located within protective personnel posts at access points. Motorized gates shall be designed to facilitate manual operation during power outages.

      (3) Access control points shall facilitate ingress and egress of emergency vehicles and fire protection equipment.

      (4) The number of access control points shall be minimized to establish and maintain the level of integrity required for that particular Security Area.

   b. Functions. The following functions shall be performed at access control points:

      (1) Provide a barrier to personnel entering Security Areas until such time as entry is requested and/or authorized.

      (2) 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.

      (3) 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.

      (4) Access from one Security Area into another Security Area with increased protection requirements shall be controlled.

2. AUTOMATED ACCESS CONTROL SYSTEMS.

   a. Equipment. A security badge may be used to electronically store information relevant to the badge and badge holder for automated access control systems. Automated access control equipment, where used, shall meet the following requirements:

(1) The probability of an unauthorized individual gaining access through normal operation of the equipment shall be documented.

(2) The probability of an authorized individual being rejected for access through normal operation of the equipment shall be documented.

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

(4) Badge readers at Material Access Areas shall be equipped with anti-passback protection.

b. Protection. Badge readers and associated equipment used for the protection of Category I and/or Category II special nuclear material, Vital Equipment, and/or classified matter shall be protected in the following manner:

(1) 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.

(2) 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.

(3) Auxiliary power shall be provided at installations where continuous service is required.

(4) The system shall record attempted unauthorized use.

(5) Access transactions which are or can be displayed, and where authorization data, badge encoded data, and personal identification or verification 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.

(6) 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.

(7) 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.

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

(9) Records reflecting active assignments of badges, personal identification numbers, levels of access, security clearances, and similar system-related records shall be maintained. Records concerning personnel removed from the system shall be retained for 1 year unless a longer period is specified by other requirements.

3. ENTRY/EXIT INSPECTIONS.

a. Inspection Equipment. Metal detectors, special nuclear material monitors, explosives detectors, and X-ray machines, as described below, may be used in lieu of or to supplement protective personnel conducting inspections for prohibited articles and Government property (e.g., special nuclear material).

(1) General.

(a) Passage of individuals, vehicles, and/or packages through a portal (e.g., walkthrough) metal detector and/or special nuclear material monitor shall be observed and controlled by protective force personnel. Hand-held and/or portable metal detectors and special nuclear material monitors, as applicable, should be available and may be used to resolve alarms.

(b) Auxiliary power should be provided to portal metal detectors and special nuclear material monitors. Hand-held detectors and monitors may be used as compensatory measures if auxiliary power is not feasible.

(c) 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.

(d) Measures shall be taken to preclude the unauthorized changing of control settings.

(e) Alarms shall annunciate audibly and visually.

(2) Portal Metal Detectors. Portal metal detectors shall meet the detection requirements established in paragraph 3b(2).

(3) Special Nuclear Material Monitors.

(a) Special nuclear material monitors shall meet detection requirements established in DOE 5633.3A.

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

(4) X-Ray Machines.

(a) X-ray machines shall be capable of imaging a 26-gauge wire at Step 5 of an American Society for Testing and Materials step wedge. (Reference American Society of Testing

Materials (ASTM) Standard 792-88, "Standard Practice for Design and Use of Ionizing Radiation Equipment for the Detection of Items Prohibited in Controlled Access Areas.")

(b) Compensatory measures shall be available at each location to provide equal detection probabilities in the event of X-ray machine failure.

b. Entry Inspection Procedures.

(1) Explosives Detection. Procedures to enforce prohibited articles requirements at page V-2, paragraph 1g(2) shall be documented. Personnel, vehicles, and packages shall be inspected at the entrances to Protected Areas and Material Access Areas. Local safeguards and security authorities may establish inspection requirements for other types of Security Areas.

(2) Metal Detection. 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.

(a) Portal metal detectors used for Protected Area entry applications shall, at a minimum, detect test weapons (b) 1 and 2 below in all locations throughout the detection field.

(b) Portal metal detectors used for Material Access Area entry applications shall, at a minimum, detect test weapons (b) 1, 2, and 3 below in all locations throughout the detection field. The following shall be used as standard test weapons:

1 Steel and aluminum alloy 0.25-caliber automatic pistol; manufactured in Italy by Armi Tanfoglio Giuseppe; sold in the United States by Excam as Model GT27B and by F.I.E. as the Titan; weight is approximately 343 grams.

2 Aluminum Model 7, 0.380-caliber Derringer; manufactured by American Derringer Corporation; weight is approximately 200 grams.

3 Stainless steel 0.22-caliber long rifle mini-revolver; manufactured by North American Arms; weight is approximately 129 grams.

(3) X-Ray. X-ray machines are considered an acceptable means of inspecting bulk and hand-carried items for prohibited articles entering Protected Areas and Material Access Areas.

c. Exit Inspection Procedures. Where required, personnel, vehicles, and hand-carried items, including packages, briefcases, purses, and lunch pails, shall be subject to exit inspections to deter and detect unauthorized removal of safeguards and security interests from applicable Security Areas. Personnel inspections for special nuclear material may be accomplished through the use of collocated special nuclear material monitors and metal detectors. Personnel inspections for classified matter or other safeguards and security interests may be accomplished by a visual inspection.

(1) Metal Detectors. 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.

(2) Special Nuclear Material Monitors. The use of special nuclear material monitors is an acceptable means of inspecting for concealed special nuclear material.

CHAPTER VIII

PROTECTION ELEMENT: BARRIERS AND LOCKS

1. BARRIERS.

   a. General. Physical barriers such as fences, walls, doors, or activated barriers shall be used to delay unauthorized access to Security Areas. Physical barriers shall serve as the physical demarcation of the Security Area.

      (1) Barriers shall be used to facilitate effective and economical use of protective personnel and to direct the flow of personnel and vehicular traffic through designated portals in a manner to permit efficient operation of access control systems.

      (2) Permanent barriers shall be used to enclose Security Areas, except during construction or transient activities, when temporary barriers may be erected. Temporary barriers may be of any height and material that effectively impedes access to the area.

      (3) Application of barriers shall provide protection with respect to the safeguards and security interests being protected.

      (4) Sound attenuation, for those areas designated for classified discussions, shall be incorporated in accordance with the Technical Surveillance Countermeasures Procedural Guide.

   b. Fencing. When used for protection purposes, fencing shall meet the construction requirements of DOE 6430.1A, GENERAL DESIGN CRITERIA, and the following:

      (1) 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.

      (2) 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.

      (3) Physical protection features shall be implemented at all locations where storm sewers, drainage swells, and site utilities intersect the fence perimeter. Unattended openings, as identified in paragraph 1h below, shall be protected.

      (4) Galvanized steel chain link fabric, consisting of a minimum of 11 gauge with mesh openings not larger than 2 inches, shall be used at Security Areas, except its use is optional at Property Protection Areas. This 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. Overall fence height, excluding barbed wire or barbed tape coil topping, shall be a minimum of 7 feet (2.13 meters). Wood fencing may be used when nonmagnetic requirements are established and to bar vision into limited personnel access areas. Solid fencing which could increase 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.

(5) The installation of vehicle barriers shall be considered where the secured perimeter borders public vehicular traffic areas.

(6) Fence lines shall be kept clear of vegetation, trash, equipment, and other objects that could impede observation.

(7) Gate hardware for security fencing shall be installed in a manner to mitigate tampering and/or removal (e.g., brazed, peened, or welded).

(8) Security fences are not required around Property Protection Areas, unless documented in the site security plan.

(9) Alternative barriers may be used in lieu of fencing if the penetration resistance of the barrier is equal to or greater than standard fencing (see (4) above).

c. Walls. Walls serving as Security Area boundaries shall meet the following requirements:

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

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

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

(4) Walls that constitute exterior barriers of Security Areas shall extend from the floor to the structural ceiling, unless equivalent means are used.

d. Ceilings and Floors. 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.

e. Doors. Doors and door jambs shall provide the necessary barrier delay rating required by the security plan. As a minimum, requirements shall include the following:

(1) 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.

(2) A sight baffle shall be used if visual access is a factor.

(3) An astragal shall be used where doors used in pairs meet.

(4) Door louvers, baffle plates, or astragals, when used, shall be reinforced and immovable from outside the area being protected.

f. Windows. The following requirements shall be applicable to windows:

(1) When primary reliance is placed on windows as physical barriers, they shall offer penetration resistance to, and evidence of, unauthorized entry into the area.

(2) Frames shall be securely anchored in the walls, and windows shall be locked from the inside or installed in fixed (nonoperable) frames so the panes are not removable from outside the area being protected.

(3) Visual barriers shall be used if visual access is a factor.

g. Unattended Openings.

(1) Physical protection features shall be implemented at all locations where storm sewers, drainage swells, and site tilities intersect the fence perimeter.

(2) Unattended openings in security barriers, which meet the following criteria, must incorporate compensatory measures such as security bars: greater than 96 inches square (619.20 square centimeters) in area and greater than 6 inches (15.24 centimeters) in the smallest dimension; and located within 18 feet (5.48 meters) of the ground, roof, or ledge of a lower Security Area; or located 14 feet (4.26 m) diagonally or directly opposite windows, fire escapes, roofs, or other openings in uncontrolled adjacent buildings; or located 6 feet (1.83 m) from uncontrolled openings in the same barrier.

h. Activated Dispensable Barriers, Deterrents, and Obscurants. Activated dispensable barriers, deterrents, and obscurants, if used, shall meet the following requirements:

(1) Obscurants shall consider spatial density versus time.

(2) Other dispensable materials shall be prudently implemented and individually evaluated for delay effectiveness.

(3) Controls and dispensers shall be protected from tampering and shall not be collocated.

i. Vehicle Barriers. Vehicle barriers shall be used to preclude, deter, and where necessary, prevent penetration into Security Areas when such access cannot otherwise be controlled.

j. 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., nonremovable hinge pins).

2. LOCKS.

a. General. The following requirements for security locks shall be applied in a graded fashion. Consideration shall be given to the safeguards and security interest being protected, the identified threat, existing barriers, and other protection measures afforded when determining which requirements to follow.

(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." This is applicable to locks purchased or installed after the date of this Manual and for replacement of damaged equipment.

(2) If a combination lock fails on any General Services Administration-approved security container or vault door, it shall be repaired or replaced with a lock that meets Federal Specification FF-L-2740 before being used to protect classified matter or Categories I and II special nuclear material.

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

(4) Key padlocks shall meet the following specifications:

(a) 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.

(b) Medium-security, key-operated padlocks shall meet the standards in Federal Specification FF-P-2827, "Padlock, Key Operated, General Field Service." Medium-security padlocks may be used to lock containers storing Category III or IV quantities of special nuclear material or classified material classified Secret and below. These locks may be used to secure perimeter gates, buildings, emergency equipment, protective personnel weapons, and other high-value Government equipment.

(c) Low-security, regular (open)-shackle, key-operated padlocks shall meet the classes and standards in Military Specification MIL-P-17802, "Padlocks and Padlock Sets, Low Security, Key Operated, Regular (Open) Shackle" or Federal Specification A-A-1927C,

"Padlock (Pin Tumbler Mechanism)." Low-security padlocks may be used to secure electrical and telephone cabinets, equipment cabinets, etc. They shall not be used to lock containers storing special nuclear material or classified matter.

(5) Key locksets shall meet American National Standards Institute Standard A156.2, "American National Standards for Bored and Preassembled Locks and Latches."

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

(7) 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 (6.35mm) in diameter, or equivalent cross section; and be secured to the repository by welding or riveting.

(8) 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 all applicable Life Safety Codes.

b. Key Management. Security keys shall be protected at the same level as the asset under protection. An inventory and accountability system shall be implemented. See "Office of Safeguards and Security Guide for Security Containers and Locking Devices," dated October 1993, for additional guidance.

CHAPTER IX

PROTECTION ELEMENT: SECURE STORAGE

1. VAULTS AND VAULT-TYPE ROOMS.

   a. Construction.

      (1) Vaults. The minimum standards required for construction of vaults, other than modular vaults, are detailed in DOE 6430.1Aand apply to all new construction, reconstruction, alterations, modifications, and repairs. Wall, floor, and roof construction shall be in accordance with nationally recognized standards of structural practice. Delay time to forcible entry provided by wall, floor, or roof shall be equal to or greater than the delay time provided by concrete poured in place, with a minimum 28-day compressive strength of 2,500 pounds per square inch (17,237 kilopascal). As an alternative to minimum concrete thickness or structural criteria specified in the following sections, activated barriers may be used to reduce construction and achieve the same delay time.

         (a) Floor and Walls. The thickness of the floor and walls must be determined by structural requirements, but may not be less than reinforced concrete 8 inches thick (20 centimeters thick). Walls shall be extended to the underside of the roof and ceiling slab above.

         (b) Roof and/or Ceiling. The roof and/or ceiling shall be a monolithic reinforced concrete slab of a thickness to be determined by structural requirements, but not less than reinforced concrete 8 inches thick (20 centimeters thick).

         (c) Vault Door and Frame Unit. The door and frame shall meet Federal Specification AA-D-600B, "Door, Vault, Security."

         (d) Miscellaneous Openings. Any miscellaneous openings, open ducts, pipes, registers, sewers, and tunnels of such size and shape as to permit unauthorized entry [in excess of 96 square inches (619.20 centimeters square) in area and over 6 inches (15.24 centimeters) in its smallest dimension] shall be equipped with barriers such as wire mesh, 9-gauge expanded metal, or rigid metal bars at least one-half inch (1.3 centimeters) in diameter, steel, and welded vertically and horizontally 6 inches (15.24 centimeters) on center. The rigid metal bars shall be securely fastened at both ends to preclude removal. 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. After installation, the annular space between the sleeve and the pipe or conduit shall be filled with lead, wood, waterproof caulking, or similar material, to give evidence of surreptitious removal.

         (e) Locks. Locks shall meet the requirements described on page VIII-4, paragraph 2.

(2) Modular Vaults. Modular vaults shall be constructed inaccordance with Federal Specification AA-V-2737, "Modular Vault Systems."

(3) Vault-Type Rooms. The minimum standards required for construction of vault-type rooms are detailed in DOE 6430.1A. The following are the minimum requirements for all new construction, reconstruction, alterations, modifications, and repairs of existing areas.

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

(b) Walls. Construction may be of materials offering resistance to, and evidence of, unauthorized entry into the area. If insert-type panels are used, a method shall be devised to prevent the removal of such panels without leaving visual evidence of tampering. Should any of the outer walls be adjacent to space not controlled by the Department of Energy the walls must be constructed of more substantial building materials, such as brick, concrete, corrugated metal, etc. If visual access is a factor, area barrier walls shall be of opaque or translucent construction.

(c) Windows. Those windows that open and are less than 18 feet (5.48 meters) from an access point (e.g., another window outside the area, roof, ledge, or door) shall be fitted with 1/2-inch (1.3 centimeters) bars that are separated by no more than 6 inches (15.24 centimeters), plus crossbars to prevent spreading, 18-gauge expanded metal, or wire mesh securely fastened on the inside. When visual access is a factor, the windows shall be closed and locked, and shall be made translucent or opaque. During nonworking hours, the windows shall be closed and securely fastened to preclude surreptitious entry.

(d) Doors. Doors shall be made of wood or metal and be of substantial construction. When windows, panels, or similar openings are used, they shall be secured with 18-gauge expanded metal or with wire mesh securely fastened on the inside. If visual access is a security concern, the windows shall be translucent or opaque. When doors are used in pairs, an astragal shall be installed where the doors meet.

(e) Door Louvers or Baffle Plates. When used, door louvers or baffle plates shall be reinforced with 18-gauge expanded metal or with wire mesh fastened inside the area.

(f) Ceilings.

1 When wall barriers do not extend to the true ceiling and a false ceiling is created, the false ceiling must be reinforced with wire mesh or 18-gauge expanded metal to serve as a true ceiling, or ceiling tile clips must be installed.

2 When wire mesh or expanded metal is used, it must overlap the adjoining walls and be secured in a manner to preclude removal without leaving evidence of tampering.

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

4 In some instances, there may be a valid justification for not erecting a solid suspended ceiling as part of the area. For example, in areas where overhead cranes are used for the movement of bulky equipment, the air conditioning system may be impeded by the construction of a solid suspended ceiling, or the height of the classified matter may make a suspended ceiling impractical. In such cases, special provisions, such as motion detection devices, shall be used to provide reasonable assurance that surreptitious entry to the area cannot be obtained by entering the area over the top of the barrier walls. The use of suspended ceilings is discouraged; however, where used, specific applications must be approved by the cognizant local Departmental authority for safeguards and security.

(g) Miscellaneous Openings. Miscellaneous openings shall meet the requirements for vaults as given in paragraph 1a(1)(d).

(h) Locks. Locks shall meet the requirements established in paragraph 2, page VIII-4.

b. Intrusion Detection Systems.

(1) Vaults. Doors, or similar type movable openings allowing access into vaults and modular vaults, shall be equipped with intrusion detection system devices. A balanced magnetic switch, or other equally effective device, shall be used on each door or movable opening to provide detection of attempted or actual unauthorized access.

(2) Vault-Type Rooms. Intrusion detection systems for vault-type rooms shall detect penetration through floors, walls, ceilings, and openings, or movement within the facility envelope, consistent with that required to remove or compromise matter within the vault-type room.

(a) Where intrusion detection system sensors are used for detection of facility envelope penetration, the openings as discussed above shall be referenced for the minimum required detectable size of penetration. The only exception is on-grade, concrete floors that do not require detection.

(b) Where intrusion detection system sensors are used for detection of movement within the facility envelope, sensor coverage shall be provided for credible pathways from the facility envelope to the matter being protected. Credible pathways shall consider visual protection and shall be documented. If the distance between the true floor (or ceiling) and the false floor (or ceiling) does not exceed 6 inches (15 centimeters), intrusion alarms are not required between the two floors (or ceilings).

(c) Doors, or similar type movable openings allowing access into vault-type rooms, shall be equipped with intrusion detection system devices. A balanced magnetic switch, or other equally effective device, shall be used on each door or movable opening to provide detection of attempted or actual unauthorized access.

c. Vault-Type Room Complex. Vault-type room criteria may be extended to multiple rooms, including an entire building. Open storage of Secret and Confidential classified matter is allowed in a vault- type room complex. The complex envelope shall meet penetration resistance, intrusion detection, and access control requirements of a vault-type room. Individuals shall be authorized for access to all safeguards and security interests within the vault-type room complex before entrance is granted, unless supplementary protective measures are employed. Requirements for a vault-type complex are listed below:

(1) Barrier requirements shall apply to the outer walls, floor, and ceiling. Outer walls shall extend from true floor to true ceiling. Interior walls may extend only to a false ceiling and/or raised floor. Interior doors, windows, and openings may exist between different work areas.

(2) The requirement to detect unauthorized access may be accomplished through direct visual observation by an individual authorized in the area or through intrusion detection sensors. Detection of inner wall penetration or motion within the vault-type complex is not required. False ceilings and raised floors are permitted.

(3) Intrusion sensors associated with walls, floors, and ceilings, which are not under constant visual surveillance but are associated with the vault-type room complex envelope, shall be activated and capable of detection at all times.

2. SECURITY CONTAINERS.

a. General.

(1) The General Services Administration establishes the national minimum standards and specifications for commercially manufactured security containers. Containers purchased after the date of this Manual shall conform to the latest General Services Administration standards and specifications.

(2) Containers physically modified are not considered approved by the General Services Administration.

b. Security Container Requirements.

(1) Test Certification Label. Security containers, cabinets, or repositories shall bear a test certification label on the inside of the locking drawer or door and shall be marked "General Services Administration Approved Security Container" on the outside of the top drawer or door.

(2) Maintenance. Maintenance information shall be maintained for all containers. A history for each security container describing damage sustained and repairs accomplished shall be retained for the life of the security container.

(3) Transfer of Security Containers. When a security container is transferred from one organization to another the custodian from the original organization shall certify, in writing, that all classified matter has been removed prior to the transfer. Certification shall be made to the organization's security office and shall include the security container's make and property tag number (or other unique identifying numbers or markings), the custodian's name and organization, and the statement "All classified matter has been removed from this(ese) security container(s) prior to transfer from my organization to (receiving organization)." The organization level at which this requirement shall apply (e.g., Division, Branch) is to be determined by the cognizant local Departmental authority for safeguards and security.

c. Emergency Procedures. Procedures shall be developed for safeguarding classified matter in emergency situations.

(1) If feasible, classified matter shall be secured in security containers and the intrusion detection system activated.

(2) If the emergency is life threatening, the health and safety of personnel shall take precedence over the need to secure classified matter. Security containers, vaults, and vault-type rooms shall be inspected on return to the facility to determine whether classified information has been compromised or if any classified matter is missing.

d. Protection of Security Containers and Combinations. Combinations shall be protected at the classification level and category of the matter being protected. A minimum number of authorized persons shall have the combination to the storage container or have access to the information stored within the security container. External markings on the security container that indicate the contents are Top Secret, Secret, or Confidential shall not be used. Security containers, vaults, and vault-type rooms used to protect safeguards and security interests shall be kept locked when not under direct supervision of an authorized individual. Padlocks, when not used to secure containers, shall be placed inside an open container or be secured to a hasp, drawer, or handle of the container to deter substitution.

e. Changing Combinations. Combinations shall be changed by an appropriately cleared authorized individual. Combinations shall be changed at the earliest practical time following:

(1) Initial receipt of a General Services Administration-approved security container or lock.

(2) Reassignment, transfer, or termination of employment of any person having knowledge of the combination, or when the Departmental access authorization granted to any such person is downgraded to a level lower than the category of matter stored, or when the Departmental access authorization has been administratively terminated, suspended, or revoked.

(3) Compromise or suspected compromise of a security container or its combination, or discovery of a security container unlocked and unattended.

f. Selection of Combination Settings. Combination numbers shall be selected at random, avoiding simple ascending or descending series such as 10-20-30 or 50-40-30. Care shall also be exercised to avoid selecting combinations of numbers that are easily associated with the person(s) selecting the combination (e.g., birthdates, anniversaries, social security numbers, or telephone extensions).

g. Security Repository Information. Applicable requirements concerning security repositories are provided below:

(1) Security Container Information. An SF-700, "Security Container Information," shall be completed for all security containers, rooms, vaults, and other approved locations for the storage of classified matter.

(a) Part 1 of the SF-700 shall be affixed to the security container to ensure high visibility. On rooms or vaults, Part 1 of the SF-700 shall be affixed to the inside of the door containing the combination lock. On security containers, it shall be placed on the inside (back front) of the locking drawer or on the front of the locking drawer, at the user's discretion.

(b) Part 2 and 2a of each completed copy of SF 700 shall be classified at the highest level of classification of the information authorized for storage in the repository and shall be forwarded to the central records for storage.

(2) Security Container Check Sheets. An integral part of the security check system shall be ensuring that classified matter has been properly stored and that security containers, vaults, or vault-type rooms have been secured. SF-702, "Security Container Checklist," shall be used to record the end-of-day security checks.

(a) SF-702 shall be used to provide a record of the names and times of the persons that have opened, closed, or checked a particular container, room, or vault holding classified information.

(b) The SF-702 shall be used in all situations requiring the use of a security container check sheet, and shall be affixed to the container or entrance to a room or vault.

(3) Activity Security Checklist. SF-701, "Activity Security Checklist," provides a systematic means of checking end-of-day activities for a particular work area (e.g., checking security containers, desks, and wastebaskets for classified matter; ensuring windows and doors are locked; ribbons for classified typewriters and automated data processing equipment have been secured; and security alarms have been activated), allowing for employee accountability in the event that irregularities are discovered. The use of SF-701 is optional; however, in situations requiring detailed end-of-day security inspections, the SF-701 shall be used.

(4) Records. Completed SF-701s and SF-702s shall be maintained according to General Record Schedule 18.

h. Damage and Repair of General Services Administration-Approved Security Containers. Neutralization of lockouts or repair of any damage that affects the integrity of a security container approved for the storage of classified information shall be accomplished only by appropriately cleared locksmiths.

CHAPTER X

PROTECTION ELEMENT: COMMUNICATIONS

1. GENERAL. Communications equipment shall be provided to aid reliable information exchange between protective personnel. The communications equipment shall meet the following requirements:

   a. 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, Secondary Alarm Station, and protected personnel dispatch point within the facility.

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

   c. Systems shall remain operable in the event of loss of primary electrical power.

2. DURESS SYSTEMS. Facilities with Protected Areas, Material Access Areas, and Vital Areas shall have duress capabilities between mobile and fixed posts and shall meet the following requirements:

   a. Activation of the duress alarm shall be accomplished in as unobtrusive a manner as practicable.

   b. Duress alarms shall not annunciate at the post initiating the duress alarm.

   c. The duress alarm for a Central Alarm Station shall annunciate at the Secondary Alarm Station or another fixed protective force post.

   d. The duress alarm for the Secondary Alarm Station shall annunciate at the Central Alarm Station or another fixed post.

   e. Mobile duress alarms shall annunciate at the Central Alarm Station, Secondary Alarm Station, or another fixed post.

3. RADIOS.

   a. A continuous electronic recording system shall be provided for all security radio traffic. The logging recorder shall be equipped with a time track and shall cover all security channels. The continuous electronic recording of security radio traffic requires the approval of the Office of IRM Policy, Plans, and Oversight or the Office of Security Affairs, as covered in DOE 1450.4, CONSENSUAL LISTENING-IN TO OR RECORDING TELEPHONE/RADIO CONVERSATIONS.

b. 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.

c. Mobile radios and base station radios shall be capable of maintaining two-way communication with the facility Central Alarm Station on the primary channel.

d. Fixed post radios, mobile radios, and portable radios, through the radio system, shall be capable of accessing operational and support channels used for security.

(1) These radios shall have sufficient power and sensitivity for two-way communications with the facility base stations on the primary channel.

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

e. Base station radios, controlled from the Central Alarm Station, shall include emergency response channels.

f. Portable radios shall contain sufficient battery capacity to operate for an 8-hour period at maximum expected duty cycle. Procedures for radio or battery exchange, or battery recharge, can be used to meet this requirement.

4. SPECIAL RESPONSE TEAM RADIO COMMUNICATIONS. Special Response Team radiocommunications equipment shall be capable of transmitting routine and emergency information. Equipment shall meet all requirements of the radio system for the rest of the facility, except that the Special Response Team two-way radio communications shall be equipped with digital encryption, meeting the requirements of DOE 5300.3D. Special Response Team radio equipment shall use channels separate from the normal operational channels.

CHAPTER XI

RESERVED

Vertical line denotes change.

CHAPTER XII

PROTECTION ELEMENT: MAINTENANCE

1. GENERAL. Security-related subsystems and components shall be maintained in operable condition. General policy and objectives are provided in DOE 4330.4B, MAINTENANCE MANAGEMENT PROGRAM. A regularly scheduled testing and maintenance program is required. System maintenance shall be applied in a graded fashion. Consideration shall be given to the interests/targets being protected, the identified threat, and other protection measures afforded. The physical protection program shall include a testing and maintenance program that encompasses security-related components and subsystems.

2. CORRECTIVE MAINTENANCE.

   a. Corrective maintenance shall be initiated within 24 hours of the indication of malfunction of site determined critical system elements for systems protecting Category I and II quantities of special nuclear material, Vital Equipment, and Top Secret matter. Compensatory measures shall be implemented immediately when any part of the critical system is out of service and shall be continued until maintenance is complete and the critical system element is back in service.

   b. Corrective maintenance shall be initiated within 72 hours of detection of a noncritical system element protecting Category I and Category II special nuclear material, Vital Equipment, and Top Secret matter. Corrective maintenance for a noncritical system protecting other assets shall be determined by local authority. The local cognizant authority for safeguards and security shall determine if compensatory measures are necessary.

3. PREVENTIVE MAINTENANCE. Preventive maintenance shall be performed on critical safeguards and security-related subsystems and components. Preventive maintenance shall, at a minimum, be performed in accordance with manufacturer's specifications and recommendations. The following system elements shall be included in a preventive maintenance program:

   a. Intrusion Detection and Assessment Systems.

   b. Central Alarm Station/Secondary Alarm Station alarm annunciators.

   c. Protective force equipment.

   d. Personnel access control and inspection equipment.

   e. Package and matter inspection equipment.

   f. Vehicle inspection equipment.

   g. Security lighting.

h. Security system-related emergency power or auxiliary power supplies.

4. MAINTENANCE PERSONNEL ACCESS AUTHORIZATION. Personnel who test, maintain, or service critical systems shall have access authorization consistent with the category of special nuclear material and/or classified matter being protected, unless such testing and maintenance is performed as bench services away from the Security Area or is performed under the supervision of an appropriately cleared, knowledgeable custodian of the system and/or critical component. Systems or critical components bench tested or maintained away from a Security Area by personnel without appropriate access authorization shall be inspected and operationally tested by qualified and cleared personnel prior to being put into service.

5. RECORDKEEPING. Records of testing shall be retained in accordance with the requirements of DOE 1324.2A.

CHAPTER XIII

PROTECTION ELEMENT: POSTING NOTICES

1. GENERAL. Selection of facilities, installations, and real property for posting of signs shall be based upon the need for supplementing other Federal statutes protecting against espionage, sabotage, or depredation of safeguards and security interests. Signs listing prohibited articles, as stated on page V-2, paragraph 1g(2), shall be posted at entrances to the Security Areas. Additional prohibited article signs may be erected at inner Security Areas as determined by the cognizant local Departmental authority for safeguards and security. Warning signs and/or notices shall be posted at entrances to areas under protection advising that physical protection surveillance equipment is operational.

2. TRESPASSING.

   a. Statutory and Regulatory Provisions.

      (1) Title 10 Code of Federal Regulations Part 860 and Section 229 of the Atomic Energy Act of 1954, as amended, prohibits unauthorized entry upon and unauthorized carrying, transporting, or otherwise introducing or causing to be introduced any dangerous weapon, explosive, or other dangerous instrument or matter likely to produce substantial injury or damage to persons or property, into or upon any facility, installation, or real property subject to the jurisdiction, administration, or in the custody of the Department of Energy. The statute provides for posting of regulations and penalties for violations.

      (2) Title 10 Code of Federal Regulations Part 1048 and Section 662 of the Department of Energy Organization Act prohibits unauthorized entry upon and unauthorized carrying, transporting, or otherwise introducing or causing to be introduced any dangerous instrument or material likely to produce substantial injury or damage to persons or property into or onto the Strategic Petroleum Reserve, its storage or related facilities, or real property subject to the jurisdiction, administration, or in the custody of the Department of Energy.

      (3) Title 41 Code of Federal Regulations Part 101-19.3 provides rules and regulations governing entry to public buildings and grounds under the charge and control of the General Services Administration.

   b. Posting Proposals. The administration of posting proposals are as follows:

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

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

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

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

(2) Contents.

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

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

c. Posting Requirements. The posting requirements are discussed below:

(1) Upon approval of the Director of Security Affairs, a notice designating the facility, installation, or real property shall be published in the "Federal Register" and shall be effective upon such publication, providing the Notices stating the pertinent prohibitions and penalties are posted.

(2) Property approved by the Director of Security Affairs for coverage under Section 229, Atomic Energy Act of 1954, as amended, shall be posted at entrances and at such intervals along the perimeter of the property to provide reasonable assurance of notice to persons who enter therein, with signs measuring at least 11 inches by 14 inches (28 by 36 centimeters).

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

CHAPTER XIV

PROTECTION ELEMENT: SECURITY BADGES AND CREDENTIALS

1. SECURITY BADGES.

   a. Standard Security Badge. These badges will be issued to DOE and DOE contractor employee who have long-term routine access to Departmental facilities. Each organization responsible for issuing security badges shall follow the specifications for the standard badge format as set forth in Attachment XIV-1. This format provides for: uniform placement of required features such as organization identification, serial number, magnetic stripe, and photograph; designated indicators for access authorizations, and other features.

   b. Foreign Visitor or Assignee Badge. (Refer to DOE 1240.2B, UNCLASSIFIED VISITS AND ASSIGNMENTS BY FOREIGN NATIONALS, for a description of the Unclassified Visits and Assignments by Foreign Nationals Program.) Badges for foreign visitors and assignees who require access to Security Areas shall adhere to the standard badge format. A distinctive marking shall be placed on the face of the badge to permit ready identification of the authorized holder as not possessing U.S. citizenship.

   c. Temporary Badges. Temporary badges may be utilized for a range of purposes including short period issuance to visitors, construction workers, and to DOE employees, DOE contractors, consultants, or assignees whose security badge has been lost, misplaced, forgotten, or stolen. The cognizant DOE authority for safeguards and security may prescribe provisions for issuance, use (e.g., supplementary photo identification), and return of temporary badges. Temporary badges do not need to conform to the standard badge format, except that they shall conform to the designated indicators for indicating access authorizations used for standard security badges. The badge shall so indicate if the individual (e.g., visitor) is not a U. S. citizen.

2. ISSUANCE AND RETURN OF SECURITY BADGES.

   a. Issuance of Security Badges. Cognizant DOE authorities for safeguards and security shall prescribe procedures for requesting and approving issuance of security badges. A DOE employee, DOE Contractor, or visitor who has been granted a DOE access authorization (see DOE 5631.2C, PERSONNEL SECURITY PROGRAM) may be issued a security badge which denotes the individual's access authorization.

   b. Individual Requirements. It is the responsibility of the individual to:

      (1) Thoroughly and accurately complete required forms and photos.

      (2) Read, view, and sign appropriate briefing material prior to receipt of a security badge.

      (3) Report a lost or stolen badge to the cognizant security office within 24 hours of discovery.

(4) Return the security badge for destruction when no longer valid or when requested by the supervisor, safeguards and security office, or protective force personnel.

c. Termination of Use. DOE security badges are the property of the Government and must be returned to the issuing office whenever an individual is transferred, terminates employment, or otherwise no longer requires the badge. Badges of departing visitors shall be recovered at the conclusion of the visit at the final security checkpoint. Once no longer needed, visitor photo badges shall be destroyed. Destruction shall be accomplished in a manner to preclude reconstruction of a badge. If destruction is not immediate, used badges shall be stored in a secure manner until they can be destroyed. Temporary visitor badges which do not include individuals photos shall be recovered and may be reissued.

3. USE OF SECURITY BADGES.

a. Appropriately coded security badges will be used and accepted as evidence of an access authorization (or security clearance). Such security badges shall be accepted for admittance to Limited and Protected Areas without a need for additional badging. Site or facility procedures may be established to require presentation of additional photo-identification media. Verification of an individual's DOE access authorization level and determination of "need-to-know" remain the responsibility of the individual or organization being visited prior to granting access to special nuclear material according to table II-1, page II-3, and/or the release of classified information.

b. Badges shall be worn conspicuously, photo side out, in a location above the waist and on the front of the body while in designated areas as set forth in Safeguards and Security Program directives and local safeguards and security directives unless prohibited by health or safety considerations.

c. Personnel shall protect assigned badges and maintain them in good condition. If a significant change in facial appearance takes place, a badge with a new photograph shall be requested by the individual, supervisor, or security official. Protective force personnel are authorized to confiscate faded, worn, or damaged badges.

d. Security awareness programs shall stress the importance of protecting security badges against loss or misuse. Badges shall not be used as a means of identification for unofficial purposes (e.g., cashing checks).

e. Headquarters, DOE Field Elements, and DOE contractors may use any unused portion of the standard badge for site-specific or organization-specific uses, such as delineation of authorized access areas. Such use must not interfere with areas reserved and/or utilized by the standard badge electronic data format.

4. TYPES OF CREDENTIALS.

a. Basic Security Credential. This credential is issued to those DOE employees whose official duties entail conducting interviews, security investigations, inquiries, inspections, and/or surveys, and is used as a supplemental form of identification.

b. Federal Officer Credential with Shield. This credential is issued to DOE employees who require firearms/arrest authority (i.e., pursuant to section 161k of the Atomic Energy Act or section 661 of the Department of Energy Organization Act) as an official function or duty. The shield is a metal, police-type badge which is issued for ready identification when conducting a Federal law enforcement function (e.g., making an arrest or conducting an investigation). Each shield shall bear a serial number imprinted on its face. The credential shall bear the shield number.

c. Transportation Safeguards Division Credential with Shield. This credential is issued to Albuquerque Operations Office, Transportation Safeguards Division nuclear materials courier employees who require firearms/arrest authority (i.e., pursuant to section 161k of the Atomic Energy Act) as an official function or duty. The shield is a metal, police-type badge which is issued for ready identification when operating in an official capacity (i.e., Transportation Safeguards Division courier function). Each shield shall bear a serial number imprinted on its face. The credential shall bear the shield number.

d. Strategic Petroleum Reserve Credential with Shield. This credential is issued to DOE contractor security police officers who require Federal firearms/arrest authority (i.e., pursuant to section 661 of the Department of Energy Organization Act for protection of the Strategic Petroleum Reserve) as a primary function or duty. The credential shall bear the contractor metal shield number. Shields for contractor protective force personnel are issued by the employing organization. Shield design shall be approved by the Strategic Petroleum Reserve Office.

e. Contractor Protective Force Officer Credential. This credential is issued to DOE contractor security police officers who require Federal firearms/arrest authority, pursuant to section 161k of the Atomic Energy Act, as a primary function or duty. The credential shall bear the contractor shield number. Shields for contractor protective force personnel are issued by the employing organization. Shield design shall be approved by the field element safeguards and security organization.

f. Technical Security Countermeasures (TSCM) Specialist Credential. This credential is issued to DOE contractor TSCM specialists that are certified by the DOE Director of Safeguards and Security as qualified TSCM specialists, and is used as a supplementary form of identification when performing TSCM services. Each credential shall bear a serial number, photo of the credentialed individual, and an expiration date.

5. ISSUANCE OF CREDENTIALS.

a. Prerequisites and Continuing Requirements. Prior to issuing a credential to an individual, verification shall be made that the individual has fulfilled any training or other qualification requirements specified for the position or duties. Credentials for individuals who fail to maintain specified training and qualification requirements for the position and duties shall be retrieved and revoked.

b. Credential Issuance Authority.

(1) The Departmental issuing authorities for the Basic Credential, the Federal Officer Credential and Shield, and Contractor Protective Force Officer Credential are the Director of Safeguards and Security, the Director, Headquarters Operations Division, and the Directors of DOE Field Element Safeguards and Security Offices.

(2) The Departmental issuing authority for the Transportation Safeguards Division Credential with Shield is the Director, Transportation Safeguards Division.

(3) The Departmental issuing authority for the Technical Security Countermeasures Specialist credential is limited to the Director of Safeguards and Security.

c. Reissuing Credentials. If a significant change in facial appearance takes place, a credential with a new photograph shall be requested by the individual, supervisor, security official, or protective force personnel. Supervisors shall report employees exhibiting significant change in facial appearance to the responsible security organization for a determination of the need of a new credential.

d. Credential Stocks. Sources of supply or inventories of blank credentials (except Strategic Petroleum Reserve and Transportation Safeguards Division stock) shall be maintained by the Office of Safeguards and Security. Requests for blank credential stock shall be made in writing to the Office of Safeguards and Security. The Director, Transportation Safeguards Division, shall maintain inventory of Transportation Safeguards Division blank credential stock and Strategic Petroleum Reserve authorities shall maintain inventory of Strategic Petroleum Reserve blank credential stock.

e. Termination of Use. DOE credentials and shields are the property of the Government and must be returned to the issuing office whenever an employee is transferred, terminates, or otherwise no longer requires the credential or shield.

6. ACCOUNTABILITY OF BADGES, CREDENTIALS, AND SHIELDS.

a. Records. Records shall be maintained by issuing offices showing the disposition of badges, credentials, and shields issued. Such records shall include, as a minimum: description and serial number of item issued; date of issuance; name, organization, and date of destruction. Records will be maintained in accordance with the requirements of Schedule 18 of the General Records Schedule.

b. Lost Badges, Credentials, and Shields. A record of missing badges, credentials, and shields shall be maintained. Personnel and/or systems controlling access to Security Areas shall be provided current information regarding missing badges in order to prevent their misuse. The loss or recovery of badges, credentials, or shields shall be reported immediately to the issuing office.

7. STORAGE OF SECURITY BADGE MATERIALS, UNISSUED BADGES, CREDENTIALS, AND SHIELDS. Stocks of badging materials, unissued security badges, credentials, and shields shall be stored in a manner assuring their protection against loss, theft, or unauthorized use.

8. TERMINATING SECURITY BADGES, CREDENTIALS, AND SHIELDS. Badges, credentials, and shields issued to employees, contractors, and other individuals shall be recovered at the final security checkpoint or earlier and the individual(s) shall be escorted from the site if circumstances or conditions indicate such action is needed. Recovered credentials shall be destroyed. Recovered shields may be retained and reissued.

9. SHIELD AND CREDENTIAL PROCUREMENT. Procurement of shields for Federal officers other than Transportation Safeguards Division personnel shall be accomplished by the Director of Safeguards and Security. Procurement of shields for contractor personnel shall be accomplished by employing organizations. Initial procurement of credential stock shall be accomplished by the Director of Safeguards and Security, except that the Transportation Safeguards Division and the Strategic Petroleum Reserve may procure unique credential stock for their needs.

**** DATABASE NOTE:
ATTACHMENT OF ATTACHMENT XIV-1 - STANDARD BADGE SPECIFICATIONS (PAGES XIV-7 AND XIV-8) IS NOT INCLUDED IN DATABASE, DUE TO ITS FORMAT.