

U.S. Department of Energy

Washington, D.C.

ORDER

DOE 5632.4

11-4-85

SUBJECT: PHYSICAL PROTECTION OF SECURITY INTERESTS

1. PURPOSE. To prescribe the Department of Energy (DOE) policies, objectives, responsibilities, and authorities for the physical protection of security interests and to establish minimum physical protection requirements and standards for such interests.
2. CANCELLATION. DOE 5632.2, PHYSICAL PROTECTION OF SPECIAL NUCLEAR MATERIALS, of 2-16-79, and DOE 5632.1, PHYSICAL PROTECTION OF CLASSIFIED MATTER, of 7-18-79.
3. SCOPE. The provisions of this Order apply to all Departmental Elements and contractors performing work for the Department as provided by law and/or contract and as implemented by the appropriate contracting officer.
4. POLICY. The Department's security interests are to be protected from theft, sabotage, and other hostile acts which may cause adverse impacts on national security, program continuity, or on the health and safety of the public. Levels of protection appropriate to particular security interests are to be provided in a graded fashion in accordance with the potential risks to national security, program continuity, and the health and safety of the public.
5. REFERENCES. See Attachment 1.
6. DEFINITIONS. See Attachment 2.
7. RESPONSIBILITIES AND AUTHORITIES.
 - a. Assistant Secretary for Defense Programs (DP-1).
 - (1) Approves and establishes policies, standards, and procedures for the physical protection of security interests.
 - (2) Authorizes security shipments outside the United States, other than those consigned to nuclear explosive test sites, after the Director of Safeguards and Security (DP-34) advises as to the adequacy of the security measures to protect such shipments.

DISTRIBUTION:
All Departmental Elements

INITIATED BY:
Office of Safeguards
and Security

- (3) Authorizes, through the Deputy Assistant Secretary for Military Application (DP-20), the transmission of classified matter which reveals or is identified as Weapon Data to the Department of Defense (DOD), to its military components and contractors or subcontractors, and to foreign governments under agreements for cooperation.
- (4) Conducts inspections and evaluations and informs the appropriate operations office managers and program managers of the results in a timely manner; coordinates with appropriate Departmental organizations to correct deficiencies including those which have a programmatic or budgetary impact.
- (5) Approves, on the recommendation of DP-34, Departmental property and facilities for "No Trespassing" posting as authorized under section 229 of the Atomic Energy Act of 1954, as amended, and authorizes for publication in the "Federal Register" a listing of the properties and facilities designated for "No Trespassing" notice.
- (6) Implements the information collection and clearance requirements contained in 5 CFR 1320 as they apply to contractors, their employees, and other members of the public from whom information is collected under the provisions of this Order.

b. Heads of Headquarters Elements shall:

- (1) In conjunction with cognizant field elements, assure that security interests under their jurisdiction are provided physical protection in accordance with the requirements of this Order.
- (2) In coordination with field elements and DP-34, provide program guidance and support to responsible field elements on actions to be taken with respect to implementation of safeguards and security programs, including exceptions to the provisions of this Order, and budgets necessary to assure that security interests under their programmatic jurisdiction are protected in accordance with this Order.
- (3) Report immediately to DP-34 any information related to an actual, attempted, or suspected act of theft, sabotage, or other hostile act involving a Departmental security interest; including losses of special nuclear material (SNM) or classified matter, or any other circumstances indicating violation of Federal law.
- (4) Require the preparation of site-specific safeguards and security plans for property over which they have programmatic responsibility, and assist in the development of such plans in coordination with cognizant operations offices and DP-34. These site-specific plans are to be consolidated into a master plan for that operations office and a copy furnished to the program office.

- (5) Require that site-specific safeguards and security plans prepared under this Order and site-specific emergency plans and procedures prepared under DOE 5500.3 be coordinated with regard to emergencies created by malevolent threats or acts.
- (6) Consult with DP-34 on questions concerning safeguards and security requirements and other matters pertaining to physical protection.
- (7) Perform reviews to evaluate safeguards and security program funding of activities under their programmatic jurisdiction.
- (8) Consult DP-34 regarding all aspects of security operations at Headquarters or for Headquarters-administered contracts.
- (9) Approve the transmittal of classified nonnuclear matter and classified documents and information, except Weapon Data, to the DOD and its military components, to other Government agencies, and to their contractors or subcontractors, and to foreign governments under agreements for cooperation.
- (10) Obtain the Assistant Secretary, Management and Administration (MA-1), support and guidance on the policy and procedures for the administration of the planning, design, and construction or alteration of facilities.
- (11) Participate in the development, review, and concurrence of Orders and standards for the safeguards and security, public health and safety, and other program interests associated with the programs under their cognizance.

c. Director of Safeguards and Security (DP-34).

- (1) Develops Orders and standards for the physical protection of Departmental security interests with the concurrence of responsible Departmental Elements.
- (2) Provides staff assistance to Heads of Departmental Elements in the development of safeguards and security plans and in the implementation of physical protection systems.
- (3) Establishes and maintains a systematic and common Departmental approach for safeguards and security resource management (including construction, operating expenses, and capital expenditures) to tie safeguards and security objectives to overall Departmental plans and programs.
- (4) Evaluates the adequacy of security measures for security shipments outside the United States, other than those consigned to nuclear explosive test sites, and advises DP-1.

- (5) Determines that appropriate corrective measures are being planned or implemented based on findings identified in inspection reports. Consults with the cognizant outlay program managers and field office managers to aid in assuring that cost-effective corrective measures are planned and implemented to meet any deficiencies identified.
- (6) Reviews and concurs in field office safeguards and security Master Plans.
- (7) Conducts research and development in physical protection technology and equipment, in consultation with the responsible program office(s) to meet present and future safeguards and security requirements.
- (8) Reviews and provides consultation to Heads of Field Elements on exceptions to the provisions of this Order with respect to the protection of Category II or greater quantities of SNM, and for other security interests subject to the protection requirements of threat guidance published by the Assistant Secretary for Defense Programs. Review and consultation will be made prior to actual implementation of the exception. (Note: Exceptions made by the field on an emergency basis may be implemented prior to review and consultation by DP-34.)
- (9) Procures and distributes to field elements inserts for employee identification badges (DOE F 5631.19).
 - (a) Issues employee identification badges at Headquarters, and security credentials at Headquarters and Field Elements.
 - (b) Maintains records of such badges for Headquarters employees.
- (10) Disseminates reports of losses and recoveries of employee identification badges.
- (11) Recommends to DP-1 for approval and subsequent publication in the "Federal Register," a listing of property and facilities designated for "No Trespassing" posting under section 229, Atomic Energy Act of 1954, as amended.
- (12) Maintains liaison with the Federal Bureau of Investigation (FBI) and other Federal law enforcement and security agencies with respect to matters of policy and tactical situations at Headquarters or in support of field office requests.
- (13) Reviews and concurs in the physical and technical security criteria for sensitive compartmented information facilities prior to initiation of new construction, and assures that physical and technical security surveys are made prior to occupancy.

- (14) Develops, in coordination with Heads of Headquarters Elements, and assures implementation of, procedures governing security requirements for Headquarters operations. (Note: Specific guidance to security requirements for Headquarters operations will be forthcoming in a Headquarters directive.)
- (15) Monitors the execution of physical protection surveys of property and facilities under the jurisdictions of field elements.
- (16) Maintains a master facility record of all security interests designated for physical protection under the requirements of this Order.

d. Deputy Assistant Secretary for Military Application (DP-20).

- (1) Administers the transportation safeguards system for domestic shipments of nuclear explosives, Category I quantities of SNM, (excluding naval reactor core shipments), classified configurations of Category II quantities of SNM as requested by responsible Heads of Field Elements, and any form of Pu-238 in excess of 5 grams. (Naval reactor core shipment program responsibility rests with the Deputy Assistant Secretary for Naval Reactors (NE-60).)
- (2) Develops and implements with the approval of DP-1, policies and procedures regarding the transmission of classified matter to DOD, its military components, their contractors or subcontractors, and foreign governments.
- (3) Reviews and coordinates with DP-34 the development of technology to protect nuclear explosives, their components, and SNM in transit.
- (4) Establishes policy and procedures for the control of weapon data.

e. Assistant Secretary, Management and Administration (MA-1), Through the Director of Project and Facilities Management (MA-22).

- (1) Develops and maintains general design criteria and construction standards for application in the planning, design, and construction or alteration of facilities. Incorporates criteria and standards for physical protection of security facilities and classified matter, with input, advice, and assistance from DP-34.
- (2) Establishes policies and procedures for the administration of the planning, design, and construction or alteration of facilities, and provides oversight guidance and evaluation of the program.

f. Assistant Secretary for Environment, Safety, and Health (EH-1).

- (1) Advises and recommends policy and standards related to personnel and environmental protection from radioactive materials and oversees all operations to assure compliance with such policy and standards.

- (2) Participates in the development of procedures and methods for implementing policies and standards for the safe transportation of SNM, other than that transported by the transportation safeguards system.
- (3) Serves as the primary point of contact with the transportation industry and with Federal, State, and local agencies in implementing the Department's transportation policies and standards for hazardous material other than nuclear explosives, SNM, or other classified matter.
- (4) Coordinates the emergency preparedness program with the physical protection program for emergencies created by malevolent threats or acts.

g. Heads of Field Elements shall:

- (1) In conjunction with cognizant Headquarters elements, assure that security interests under their jurisdictions are provided physical protection in accordance with the requirements of this Order.
- (2) Participate in the development, review, and concurrence of Orders and policy standards for the safeguards and security, public health and safety, and other security interests under their jurisdiction.
- (3) Obtain:
 - (a) From the Manager, Nevada Operations Office, approval for the release of security shipments to nuclear explosive test sites outside the United States.
 - (b) From DP-20, approval for the transmission of classified matter revealing or identified as Weapon Data to the DOD, its military components, and its contractors and subcontractors.
- (4) Take such action as may be appropriate to assure physical protection of security interests, including curtailment and suspension of operations when, in their judgment, such operations would result in an undue risk to national security, program continuity, or the health and safety of the public. Curtailment or suspension of operations shall be coordinated with the responsible outlay program manager and DP-34.
- (5) Request DP-34 to evaluate and advise DP-1 as to the adequacy of security measures for transporting security shipments outside the United States, other than those consigned to nuclear explosive test sites.
- (6) Authorize, pursuant to section 161k of the Atomic Energy Act of 1954, as amended, the carrying of firearms and the making of arrests without warrant by Departmental couriers and other DOE and DOE contractor and subcontractor protective force personnel as necessary in the performance of official duties.

- (7) Coordinate security shipments with other Heads of Field Elements.
- (8) Approve, as appropriate, manuals and instructions prepared by contractors or subcontractors to implement the provisions of this Order.
- (9) Advise DP-34 and request assistance if site-specific considerations dictate that the protection system include components for which no test data are available.
- (10) When site or program considerations make the strict implementation of this Order infeasible, then an alternate approach to providing equivalent levels of physical protection shall be developed and forwarded to DP-34 and the responsible program office for review and consultation. Exceptions concerning the physical protection of SNM in Category II or greater quantities need to be forwarded for review and consultation prior to implementation. DP-34 will also review and consult on exceptions that affect the protection afforded other security interests subject to threat guidance published by DP-1. All other exceptions to the requirements of this Order may be implemented at the discretion of the Heads of Field Elements.
- (11) Issue employee identification badges and maintain records of all such badges.
- (12) Report losses and recoveries of identification badges promptly to DP-34.
- (13) Approve the holding of classified conferences outside approved security areas and advise DP-34.
- (14) Perform planning for funding and staffing to implement this Order, including the preparation and approval of site-specific safeguards and security plans for each facility, the operations office, and an overall operations office master plan. These plans will be furnished to the program offices involved.
- (15) Maintain liaison with the FBI and local law enforcement agencies and establish, document, and test, as appropriate, the support to be expected from the FBI and local law enforcement agencies in response to security incidents.
- (16) Require testing of the physical protection system to verify the maintenance of a continuing high state of effectiveness against the threat spectrum delineated both in this Order and also in separate, classified guidance issued periodically by DP-34.
- (17) Report annually, on 12-1, to the Office of the Secretary, with copies to DP-1, the Inspector General (IG-1), outlay program managers, and DP-34, on the state of safeguards and security of security interests under their respective jurisdiction.

- (18) Recommend to DP-34 for publication in the "Federal Register" a listing of property and facilities designated for "No Trespassing" posting under section 229, Atomic Energy Act of 1954, as amended.
- (19) Assure that "No Trespassing" notices are posted.
- (20) Assure that employees are made fully aware of and understand their responsibilities for protecting security interests and that contractors have formulated adequate plans for promptly notifying and requesting assistance from city, county, and State police departments and other law enforcement officials if security interests are threatened by theft, sabotage, or other hostile acts.
- (21) Approve the transmittal of classified nonnuclear matter and classified documents and information, except Weapon Data, to the DOD and its military components, to other government agencies, and to their contractors or subcontractors.
- (22) Determine which byproducts of source materials or special nuclear materials may be designated as scrap (recoverable) or waste (not recoverable) for physical protection purposes.
- (23) Report immediately to DP-34 any information related to an actual, attempted, or suspected act of theft, sabotage, or other hostile act involving a security interest, including losses of SNM or classified matter, or any other circumstances indicating violation of Federal law.
- (24) Consult with DP-34 on questions concerning safeguards and security requirements and other matters pertaining to physical protection.
- (25) Determine, based on the advice of the designated physician, that a security inspector or guard may be retained in an active status for the effective performance of normal and emergency duties.
- (26) Prepare reports on expenditures for safeguards and security activities and provide copies of these reports to DP-34 and outlay program managers.
- (27) Inform outlay program managers and DP-34 of requirements for new or additional funds to satisfy minimum Departmental Order requirements and/or to correct site-specific vulnerabilities.
- (28) Conduct surveys of the facilities under their cognizance in accordance with DOE 5634.1.
- (29) Request MA-1 to provide support and guidance on the policy and procedures for administration of the planning, design, construction, or alteration of facilities.
- (30) Report promptly, within 24 hours, to DP-34 serious or major incidents involving the use of firearms, including accidental discharge, or any serious incident involving an arrest or detention.

- (31) Report, in accordance with DOE 5000.3, all discharges of firearms and other weapons other than those normally expected during training exercises.
- (32) Assure that safeguards and security plans and emergency plans and implementing procedures are coordinated and appropriately integrated to assure proper response to emergencies created by malevolent threats or acts.

h. Manager, Albuquerque Operations Office.

- (1) In addition to the responsibilities outlined on page 6, paragraph 7g, manages the transportation safeguards system for domestic shipment of nuclear explosives; Category I quantities of SNM, excluding naval reactor core shipments; classified configurations of Category II quantities of SNM as requested by responsible outlay program managers; and any form of Pu-238 in excess of 5 grams. Naval reactor core shipment responsibility rests with the Pittsburgh Naval Reactors Office.
- (2) Conducts surveys of security shipments under his or her jurisdiction or requests another Departmental Element to conduct such surveys.
- (3) Submits reports of such surveys to DP-34 and appropriate program managers.
- (4) Operates SECOM, the nationwide security communications system, in support of the transportation safeguards system.
- (5) Assures that job-related qualification requirements, approved by the Office of Personnel Management, for application to Transportation Safeguards Division couriers are carried out, consistent with applicable laws, regulations, and Departmental policy.

i. Manager, Nevada Operations Office.

- (1) Deploys necessary classified matter in support of the nuclear emergency search team mission. Classified matter may be deployed outside the United States in connection with the mission.
- (2) In addition to the responsibilities outlined in paragraph 7g, approves the release of security shipments involving nuclear test devices between the Department and domestic military installations within, and nuclear explosive test sites outside, the United States. The commander of the task force assigned to conduct overseas nuclear explosive tests also has this authority.

j. Manager, Oak Ridge Operations Office. In addition to the responsibilities outlined in paragraph 7g, has safeguards and security responsibility for the Office of Scientific and Technical Information. This includes oversight for physical, communications, personnel, and automated data processing security.

- k. Managers of the Albuquerque, Nevada, Oak Ridge, San Francisco, and Savannah River Operations Offices. In addition to the responsibilities outlined in paragraphs 7g, h, i, and j, above, as applicable, approve the transmission of classified matter revealing or identified as Weapon Data to DOD, its military components, its contractors or subcontractors, or to foreign governments under agreements for cooperation, upon specific delegation of authority by DP-1 through DP-20.
- l. Deputy Assistant Secretary for Naval Reactors (NE-60).
- (1) Administers the Naval Nuclear Propulsion Program including oversight of program support for security activities of Headquarters, Pittsburgh Naval Reactors Office, Schenectady Naval Reactors Office, together with Naval Reactors prototype sites (Kesselring, Windsor, Naval Reactors Facility).
 - (2) Requests assistance from Defense Programs and appropriate operations office activities as necessary to assure that the requirements of this Order are met.

BY ORDER OF THE SECRETARY OF ENERGY:



WILLIAM S. HEFFELFINGER
Director of Administration

REFERENCES

1. Atomic Energy Act of 1954 (42 U.S.C. 2201k), 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 14, "General Authority," section 161, "General Provisions," which sets forth the authority necessary to perform the functions of the Department and the Nuclear Regulatory Commission.
 - c. Chapter 18, "Enforcement," sections 221-233, which sets forth the authority necessary to protect Restricted Data and to safeguard property and establish criminal penalties for violation of provisions of the Atomic Energy Act.
 - d. Chapter 18, "Enforcement," section 229, "Trespass Upon Commission Installations," which sets forth the authority to issue regulations and establishes penalties for violating these regulations relating to the entry upon or carrying, transporting, or otherwise introducing or causing to be introduced any dangerous weapons, explosive, or other dangerous instrument or material likely to produce substantial injury or damage to persons or property, into or upon any facility, or installation, or real property of the Department or the Nuclear Regulatory Commission.
2. DOE "Classification Guide" (CG-SS-1) and "Classified Supplement," of 3-81, which provide original classification determinations for National Security Information (NSI) about the safeguarding of nuclear materials and provide guidance for derivatively classifying documents and materials containing such NSI, Restricted Data, and/or Formerly Restricted Data.
3. DOE "COMSEC Procedural Guide," of 2-28-83, which provides information and instructions on communications and logistical aspects of the Department's secure communications activities, and identifies the other publications applicable to communications security activities of the Department and Departmental contractors.
4. DOE Procedural Guide, "Security Standards For Sensitive Compartmented Information And Facilities," of 8-2-84, which establishes procedures and construction criteria for sensitive compartmented information facilities and includes operating procedures and Departmental policy for the control, handling, accountability, and dissemination of sensitive compartmented information within the Department.
5. "Generic Threats for DOE Nuclear Programs and Facilities," of 1-31-83, issued by the Assistant Secretary for Defense Programs, which identifies and characterizes the range of potential generic adversary threats to the Department's nuclear programs and facilities which could adversely impact national security and the health and safety of the public.

6. Title 5 Code of Federal Regulations (CFR), Part 1320, Paperwork Reduction Act, which directs the identification and clearance of information collections levied on the public, including contractors, State and local government units, and persons who perform services for the Department on an individual basis.
7. 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 the Department.
8. Title 10 CFR Part 1046, Defense Programs, Physical Protection of Security Interests; General, Protective Force Personnel, which provides medical and physical fitness qualification standards for Departmental contractor employees at Government-owned facilities, whether or not privately operated.
9. Title 10 CFR Part 1047, Defense Programs: Limited Arrest Authority and Use of Force by Protective Force Officers, which establishes policy concerning arrests and associated use of force by all DOE and DOE contractor employees engaged in nuclear security duties.
10. Title 14 CFR Part 108, Airplane Operator Security, which provides requirements for the carriage of weapons and escorted persons while aboard an airplane.
11. 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.
12. Title 41 CFR Part 109, Department of Energy Property Management Regulations, which establishes a system and describes procedures for promulgating Departmental Property Management Regulations within the Federal Property Management Regulations System (FPMR) as cited in 41 CFR 101.
13. Title 18, United States Code, section 1001, "Crimes and Criminal Procedures," which provides penalties for knowingly and willfully falsifying, concealing, or covering up by any trick, scheme, or device, a material fact, or makes any false, fictitious, or fraudulent statement or entry.
14. DOE 1321.1B, DEPARTMENTAL DIRECTIVES SYSTEM, of 4-7-83, which establishes the permanent directives system for the Department that shall be used for publishing directives issued by Headquarters, and addressed to Departmental Elements.
15. DOE 1360.2, COMPUTER SECURITY PROGRAM FOR UNCLASSIFIED COMPUTER SYSTEMS, of 3-9-79, which establishes policies and procedures for developing, implementing, and administering a program for safeguarding Departmental computer systems and in particular the Department's sensitive unclassified information.

16. DOE 5000.3, UNUSUAL OCCURRENCE REPORTING SYSTEM, of 11-7-84, which provides criteria and instructions for reporting unusual occurrences that have programmatic significance at Departmental operations.
17. DOE 5300.2A, TELECOMMUNICATIONS: EMISSION SECURITY (TEMPEST), of 8-30-82, which establishes the telecommunications program for emission security and implements the provisions of the national policy that are applicable to emission security.
18. DOE 5300.3A, TELECOMMUNICATIONS: COMMUNICATIONS SECURITY, of 12-7-83, which establishes policy and provides guidance concerning the communication security aspects of Departmental telecommunication services and implements the National Telecommunications Protection Policy.
19. DOE 5300.4A, TELECOMMUNICATIONS: PROTECTED DISTRIBUTION SYSTEMS, of 9-28-84, which establishes policy for protected distribution systems used to process classified or sensitive unclassified information related to national security.
20. DOE 5480.1A, ENVIRONMENTAL PROTECTION, SAFETY, AND HEALTH PROTECTION PROGRAM FOR DOE OPERATIONS, of 8-31-81, which establishes the Departmental Environmental Protection, Safety, and Health Protection Program.
21. DOE 5484.1, ENVIRONMENTAL PROTECTION, SAFETY, AND HEALTH PROTECTION INFORMATION REPORTING REQUIREMENTS, of 2-24-81, which establishes the requirements and procedures for the reporting of information having environmental protection, safety, or health protection significance for Departmental operations.
22. DOE 5500.2, EMERGENCY PLANNING, PREPAREDNESS, AND RESPONSE FOR OPERATIONS, of 8-13-81, which establishes policy, assigns responsibilities and authorities, and provides guidance for the emergency planning, preparedness, and response to operational emergencies in which there is a potential for the destruction of property, theft, or release of radioactive material, including terrorist threats or acts.
23. DOE 5500.3, REACTOR AND NONREACTOR NUCLEAR FACILITY EMERGENCY PLANNING, PREPAREDNESS, AND RESPONSE PROGRAM FOR DEPARTMENT OF ENERGY OPERATIONS, of 8-13-81, which establishes requirements for site-specific emergency plans and procedures for radiological emergencies (including malevolent threats or acts) occurring in Departmental reactor and nonreactor nuclear facilities.
24. DOE 5560.1A, PRIORITIES AND ALLOCATIONS PROGRAM, of 5-8-85, which establishes policies and procedures for the administration of the Department's priorities and allocations program for industrial products, materials, and services.
25. DOE 5630.2, CONTROL AND ACCOUNTABILITY OF NUCLEAR MATERIALS, BASIC PRINCIPLES, of 8-21-80, which contains the basic principles and requirements for control and accountability of all nuclear materials.
26. DOE 5633.1, VIOLATIONS OF LAWS, LOSSES, AND INCIDENTS OF SECURITY INTEREST, of 7-28-80, which sets forth Departmental procedures to assure timely and effective investigation and other followup action relating to violations of Federal laws and to certain losses of security interest.

27. DOE 5634.1, SECURITY SURVEY AND FACILITY APPROVAL, of 5-2-83, which establishes Departmental requirements for the conduct of periodic onsite security surveys of classified facilities under the Department's jurisdiction. The Department shall assure that all facilities eligible to receive, process, reproduce, store, transmit, or handle classified matter, including special nuclear material, have been granted facility approval prior to permitting access to such matter or material.
28. DOE 5635.1, CONTROL OF CLASSIFIED DOCUMENTS AND INFORMATION, of 11-24-80, which provides guidance relative to the safeguarding and control of classified documents and information.
29. DOE 5636.2, SECURITY REQUIREMENTS FOR CLASSIFIED AUTOMATIC DATA PROCESSING SYSTEMS, of 1-10-80, which establishes uniform requirements, policies, and responsibilities for the development and implementation of a program to assure the security of information stored in classified automatic data processing systems.
30. DOE 5636.3, TECHNICAL SURVEILLANCE COUNTERMEASURES PROGRAM, of 1-27-82, which establishes the Technical Surveillance Countermeasures Program.
31. DOE 5636.4, SECURITY MANUAL FOR CLASSIFIED AUTOMATED DATA PROCESSING SYSTEMS, of 7-13-83, which establishes uniform procedures for techniques to be used when applying computer security measures for the protection of classified information being processed, stored, or produced on automatic data processing systems.

DEFINITIONS

1. CATEGORY I QUANTITIES OF SPECIAL NUCLEAR MATERIAL.

- a. Uranium-235 (contained in Uranium enriched to 20 percent or more in the isotope U-235) alone, or in combination with Plutonium and/or Uranium-233 when (multiplying the Plutonium and/or Uranium-233 content by 2.5) the total is 5,000 grams or more.
- b. Plutonium and/or Uranium-233 when the Plutonium and/or Uranium-233 content is 2,000 grams or more.
- c. SNM in lesser quantities but which is located in the same area or shipment with other SNM with which it could be selectively combined to produce the equivalent quantities specified in paragraph 1a of this category. 1/

2. CATEGORY II QUANTITIES OF SPECIAL NUCLEAR MATERIAL.

- a. Uranium-235 (contained in Uranium enriched to 20 percent or more in the isotope U-235) alone, or in combination with Plutonium and/or Uranium-233 (multiplying the Plutonium and/or Uranium-233 content by 2.5) when the total is 1,000 to 4,999 grams.
- b. Plutonium and/or Uranium-233 when the Plutonium and/or Uranium-233 content is 400 grams to 1,999 grams.
- c. SNM in lesser quantities but which is located in the same area or shipment with other SNM with which it could be selectively combined to produce the equivalent quantities specified in paragraph 2a of this category. 1/

3. CATEGORY III QUANTITIES OF SPECIAL NUCLEAR MATERIAL have been further divided into two subcategories IIIA and IIIB.

a. Category IIIA Quantities of Special Nuclear Material.

- (1) Uranium-235 (contained in Uranium enriched to 20 percent or more in the isotope U-235) when the total is 350 grams to 999 grams.
- (2) Plutonium and/or Uranium-233 when the Plutonium and/or Uranium-233 content is 220 grams to 399 grams.

1/ DOE 5630.2 provides a Category IA and IB, this Order provides a Category IIIA and IIIB. Reconciliation of these facts, particularly as it relates to accumulation of special nuclear materials (rollup) will be provided in future guidance from the Office of Safeguards and Security.

- (3) Combination of Plutonium and/or Uranium-233 with Uranium-235 (contained in Uranium enriched to 20 percent or more in the isotope U-235) when the total is less than 1,000 grams and the Plutonium and/or Uranium-233 content is less than 400 grams.
- (4) SNM in lesser quantities but which is located in the same area or shipment with other SNM with which it could be selectively combined to produce the equivalent quantities specified in paragraph 3a(1). 1/

b. Category IIIB Quantities of Special Nuclear Material.

- (1) Uranium 235 (contained in Uranium enriched to 20 percent or more in the isotope U-235) when the total of the U-235 content is 1 gram to 349 grams.
- (2) Plutonium and/or Uranium-233 when the Plutonium and/or Uranium 233 content is from 1 gram to 219 grams.
- (3) Uranium-235 contained in Uranium enriched to less than 20 percent in the isotope U-235 in all quantities 1 gram and above.

4. CLASS A FACILITY designates a facility which is:

- a. Judged to be engaged in administrative activities considered to be essential to the direction and continuity of the overall program. Such judgment is rendered by Heads of Field Elements;
- b. Engaged in research and development, manufacture, production, assembling or storage of nuclear weapons, weapon assemblies, or military reactors;
- c. Engaged in major research and development in uranium enrichment or operation of major uranium enrichment facilities;
- d. Involved in research and development, manufacture or production, and assembling of nonnuclear weapon components, assemblies, and parts essential to the weapons or military reactors programs;
- e. Receiving, handling, and storing Top Secret documents exclusive of keying material for secure communications over an extended period; or
- f. A possessor of Category I quantities of special nuclear material.

1/ DOE 5630.2 provides a Category IA and IB, this Order provides a Category IIIA and IIIB. Reconciliation of these facts, particularly as it relates to accumulation of special nuclear materials (rollup) will be provided in future guidance from the Office of Safeguards and Security.

5. CLASS B FACILITY designates a facility which is a:
 - a. Departmental contractor or subcontractor facility or Government-owned facility with security interests other than the type categorized for Class A facilities and which handles and stores Secret Weapon Data documents or Secret research and development reports;
 - b. Facility, other than the type categorized for Class A facilities, in the uranium enrichment program;
 - c. Facility in possession of Category II quantities of SNM;
 - d. Departmental National laboratory with security interests other than the type categorized for Class A facilities; or
 - e. Emergency operations centers. (Unmanned Emergency Operations Centers are considered Class C facilities.)
6. CLASS C FACILITY designates a facility which is a:
 - a. Federal Records Center holding classified security interests of the Department;
 - b. A Departmental contractor, or subcontractor facility engaged in manufacturing, research and development, administrative or consultant activities, including machine and specialty shops, automatic data processing, printing and photographic work, and design engineering where the security interests are limited in scope;
 - c. Facility established for classified bid negotiations or quotations; or
 - d. Facility authorized to retain classified matter, other than that noted under Classes A and B above, after completion or termination of contract, subcontract, or other agreement.
7. CLASSIFIED INFORMATION. Top Secret, Secret, and Confidential Restricted Data, Formerly Restricted Data, and National Security Information, for which the Department is responsible and which requires safeguarding in the interest of national security and defense.
8. CLASSIFIED INTEREST. Classified documents, information, or material including classified SNM possessed by the Department, a contractor of the Department, a Departmental facility, or any other facility under the Department's jurisdiction.
9. CLASSIFIED MATTER. Classified information, documents, parts, components, or other material.

10. CLASSIFIED TELECOMMUNICATIONS FACILITY. A facility which contains both crypto equipment and input/output equipment for the electronic transmission, receipt, or processing of classified information. The crypto equipment and input/output equipment may either be installed in the same area and share common security measures or installed in different parts of the same security area connected by a protected distribution system, with each area having its own security measures.
11. CONFIDENTIAL. A classification level which is applied to classified matter, the unauthorized disclosure of which could be expected to cause damage to the national security.
12. CONTRACTOR. As used in this Order, the term "contractor" includes subcontractors, vendors, consultants, bidders, recipients of financial assistance agreements, and another Federal agency in the case of interagency acquisition.
13. CUSTODIAN. Any person having assigned responsibility for the control and accountability of classified matter.
14. CRYPTO. A designation or marking applied to classified and unclassified telecommunications keying material indicating that it requires special accounting and safeguarding.
15. DEPARTMENTAL-APPROVED EQUIPMENT. Equipment (e.g., alarm, assessment, monitoring, detection) used in conjunction with all other elements of a site-specific safeguards and security system as described in the site-specific safeguards and security plan (after such plan is approved by the Departmental element).
16. DEPARTMENTAL PROPERTY. All land, buildings, and structures (real property) and portable equipment, records, and supplies (personal property) which are owned by the U.S. Government or rented or leased by the U.S. Government from commercial sources and are subject to the administrative custody or jurisdiction of the Department.
17. DURESS SYSTEM. A system which can covertly communicate a situation of duress to a security control center or other personnel who can notify a security control center.
18. EXCLUSION AREA. A security area for the protection of classified matter where mere access to the area would result in access to classified matter.
19. FACILITY. An educational institution, manufacturing plant, laboratory, or office building utilized by the Department or its contractors or subcontractors for the performance of work under the jurisdiction of the Department.
20. FIELD ELEMENT. Any Departmental organizational component located outside the Washington, DC, metropolitan area.

21. FORMERLY RESTRICTED DATA. Classified information jointly determined by the Assistant Secretary for Defense Programs and the Department of Defense (DOD) to be related primarily to the military utilization of atomic weapons, and removed by the Assistant Secretary for Defense Programs from the Restricted Data category pursuant to section 142(d) of the Atomic Energy Act.
22. GUARD. An unarmed Departmental contractor individual who is employed for, and charged with, the protection of classified matter or Government property.
23. HEADQUARTERS STAFF. Refers to Heads of Headquarters Elements and employees under their respective jurisdictions.
24. HEADS OF HEADQUARTERS ELEMENTS. Refers to the Office of the Secretary, Secretarial Officers, and DOE Staff Officers.
25. INCIDENT REPORT. A report of any theft or attempted theft of Government-owned property, or threatened, actual, or attempted arson, civil disorders, riots, sabotage, terrorism, or vandalism affecting facilities or property owned by or contracted to the Department.
26. ISOLATION ZONE. An area surrounding a protected facility which has been cleared of any objects which could conceal vehicles or individuals, and which affords unobstructed observation of, or other means of detection of, entry into the area.
27. INTRUSION ALARM SYSTEM (PERIMETER OR INTERIOR). Detection hardware and/or software comprised of: sensors; alarm assessment systems; and alarm reporting systems (including alarm communications and information display equipment).
28. LIMITED AREA. A security area for the protection of classified matter where guards, security inspectors, or other internal controls can prevent access by unauthorized persons to classified matter.
29. MATERIAL. Any raw, in-process, or manufactured commodity, equipment, component, accessory, part, assembly, or product of any kind.
30. MATERIAL ACCESS AREA. An area which contains a Category I quantity of SNM and is specifically defined by physical barriers, located within a protected area, and subject to specific access controls.
31. MATERIAL SURVEILLANCE PROCEDURES. Procedures to assure the observation of an area containing SNM by at least two cleared and knowledgeable authorized persons who may be doing other work but who can give an alarm in time to prevent the unauthorized removal or diversion of the SNM or an act of sabotage involving SNM. One of the persons who maintains such surveillance must be "Q" cleared, and the other must possess at least an "S" or "L" access authorization unless the surveillance entails access to Secret Restricted Data, in which case the other person must also possess a "Q" access authorization. If the surveillance entails access to Confidential Restricted Data, then an "L" access authorization is required. (Note: Refer to Chapter VI for SNM storage requirements.)

32. MATTER. Documents, information, or material.
33. NATIONAL SECURITY INFORMATION. Information that has been determined pursuant to Executive Order 12356, "National Security Information," or any predecessor order, to require protection against unauthorized disclosure and is so designated.
34. NEED-TO-KNOW. A determination by persons having responsibility for classified information or matter that a proposed recipient's access to such classified information or matter is necessary in the performance of their official or contractual duties of employment under the cognizance of the Department.
35. OUTLAY PROGRAM MANAGERS. Headquarters officials who have lead line responsibility for the execution of authorized programs with appropriated funds.
36. PERSONAL PROPERTY. Generally, movable items, that is, those not permanently affixed to and a part of the real estate. Generally, but with exceptions, items remain personal property if they can be removed without serious injury either to the real estate or to the items themselves.
37. PHYSICAL PROTECTION FACILITY. A facility, other than a security facility, which contains property owned, leased, or contracted by the U.S. Government for the use of the Department, its contractors and subcontractors, and in which significant monetary value, national security, program continuity, or protection of the public health and safety constitutes an important responsibility of the Department.
38. PROPERTY PROTECTION AREA. An area set aside for the protection of property as required by this Order.
39. PROTECTED AREA. An area encompassed by physical barriers (e.g., walls or fences), subject to access controls, surrounding a material access area or containing Category II SNM, and which meets the standards of this Order.
40. PROTECTIVE PERSONNEL. Guards, security inspectors, couriers, authorized escorts, and personnel assigned to protective details, who are employed to protect the security interests of the Department.
41. RANDOM PATROL. A patrol conducted in a manner such that the location of the patrol at any specific time cannot be predicted.
42. REAL PROPERTY. Real property includes land, improvements on the land, or both, including interests therein. The chief characteristics of real property are its immobility and tangibility. It comprises land and all things of a permanent and substantial nature affixed thereto, whether by nature or by the hand of man. By nature is meant trees, the products of

the land, natural resources; by the hand of man, those objects--buildings, fences, bridges--which he erects upon the land. All equipment or fixtures which are installed in a building in a more or less permanent manner, such as plumbing, electrical, heating, built-in cabinets, and elevators, usually are held to be part of the real estate.

43. RELATIVE INCAPACITATION INDEX. An index of the performance of commercially available ammunition and weapons as it concerns the effectiveness of the cartridge to incapacitate.
44. REMOTE INTERROGATION POINTS. Locations for receiving information (e.g., printouts) transmitted by automatic data processing centers.
45. RESTRICTED DATA. All data concerning: design, manufacture, or utilization of atomic weapons; production of special nuclear material; or use of special nuclear material in the production of energy; but shall not include data declassified or removed from the Restricted Data category pursuant to section 142 of the Atomic Energy Act.
46. SABOTAGE.
 - a. Industrial. Any deliberate act which is directed against a facility, property, component, or procedure and intended to cause damage, obstruct productivity, or interrupt normal operating functions.
 - b. Radiological. Any deliberate act directed against an SNM facility, an SNM or weapon security shipment, or a component of such facility or shipment which could directly or indirectly endanger the public health and safety by exposure to radiation.
47. SAFEGUARDS. An integrated system of physical protection, material accounting, and material control measures designed to deter, prevent, detect, and respond to unauthorized possession, use, or sabotage of special nuclear materials. In practice, safeguards involve the development and application of techniques and procedures dealing with the establishment and continued maintenance of a system of activities including physical protection, quantitative knowledge of the location and use of special nuclear materials, and administrative controls and surveillance to assure that procedures and techniques of the system are effective and are being carried out. Safeguards include the timely indication of possible diversion or credible assurances by audits and inventory verification that no diversion has occurred.
48. SCRAP. The economically recoverable byproducts of source materials or special nuclear materials, which are generated during chemical and mechanical processing, or economically recoverable fragments or portions of

any nuclear materials which may require one or more forms of chemical or physical treatment before it can be used as feed to a refinery or to a production of fuel fabrication process. Scrap is unsuitable for use as a finished product.

49. SECOM. The high frequency radio communications network operated by the Albuquerque Operations Office in support of transportation safeguards.
50. SECRET. The classification level applied to classified matter, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.
51. SECURE COMMUNICATIONS CENTER. A security area devoted in whole or in part to the encryption and decryption of sensitive and/or classified information.
52. SECURITY. Activities through which the Department defines, develops, and implements its responsibilities under the Atomic Energy Act of 1954, as amended, Federal statutes, Executive orders, and other directives, for the protection of Restricted Data and other classified information or matter, nuclear weapons and nuclear weapon components, and for the protection of Department and Departmental contractor facilities, property, and equipment. Security is also applied to special nuclear materials. When physical, personnel, and technical security are combined with material control and material accountability, the protection is referred to as safeguards.
53. SECURITY AREA. A physically defined space containing a Departmental security interest and subject to physical protection and access controls.
54. SECURITY CONTAINER.
 - a. A metal security container approved by the General Services Administration (GSA) for the storage of classified matter and marked "General Services Administration Approved Security Container." This container meets the acceptable minimum GSA class standards.
 - b. A burglar-resistant cabinet or chest having a body of steel at least 1/2-inch thick and a combination locked steel door at least 1-inch thick, exclusive of bolt work and locking devices.
55. SECURITY FACILITY. Any facility which has been approved by the Department for generating, receiving, using, processing, storing, reproducing, transmitting, destroying, or handling SNM or classified matter.
56. SECURITY INSPECTOR. A uniformed Departmental contractor person who is employed for, and charged with, the protection of classified matter, special nuclear material, or other Government property and who is authorized under section 161k of the Atomic Energy Act of 1954, as amended, or other statutory authority to carry firearms and to make arrests without warrant.

57. SECURITY INTEREST. A security interest includes any of the following which requires special protection: classified matter, special nuclear material, security shipments, secure communications center, sensitive compartmented information facilities, automatic data processing centers, or other systems including classified information, or Departmental property.
58. SECURITY SHIPMENT. A shipment between security areas or facilities and consisting of classified matter or special nuclear material.
59. SENSITIVE COMPARTMENTED INFORMATION. As used in this Order, sensitive compartmented information means all classified information and materials bearing intelligence community special access controls formally limiting access and dissemination. Sensitive compartmented information does not include Restricted Data as defined in the Atomic Energy Act of 1954, as amended.
60. SENSITIVE COMPARTMENTED INFORMATION FACILITY. An accredited area, room, group of rooms, or installations where sensitive compartmented information may be stored, used, and/or electronically processed.
61. SITE-SPECIFIC SAFEGUARDS AND SECURITY PLAN. A specific description of the systems and procedures implemented and planned to protect Departmental security interests and other property. The format for site-specific safeguards and security plans may be obtained from DP-34.
62. SOURCE MATERIAL. Pursuant to the provisions of section 61 of the Atomic Energy Act of 1954, as amended, source material means uranium, thorium, or any other material which is determined to be source material, or ores containing one or more of the foregoing materials in such concentration as may be determined by regulation from time to time.
63. SPECIAL NUCLEAR MATERIAL. Plutonium, uranium enriched in the isotope 233 or in the isotope 235, and any other material which is determined to be SNM, pursuant to section 51 of the Atomic Energy Act of 1954, but does not include source material, or any material artificially enriched by any of the foregoing, but does not include source material.
64. SPECIAL NUCLEAR MATERIAL FACILITY. An educational institution, a plant, Laboratory, office, or building utilized by the Department, its contractors, subcontractors, or consultants and which contains SNM.
65. SPECIAL NUCLEAR MATERIAL FACILITY APPROVAL. A determination based upon a satisfactory review of a safeguards and security plan and an onsite survey by the responsible operations office that a facility is approved to receive, use, process, and/or store SNM.

66. SPECIAL NUCLEAR MATERIAL VAULT. A penetration-resistant, windowless enclosure which has: (a) walls, floor, and ceiling substantially constructed of materials which afford forced penetration resistance at least equivalent to that of 8-inch thick reinforced concrete; (b) any openings greater than 96 square inches in area and over 6 inches in the smallest dimension protected by imbedded steel bars at least 5/8 inches in diameter on 6-inch centers both horizontally and vertically; (c) a built-in combination locked steel door which in existing structures is at least 1-inch thick exclusive of bolt work and locking devices and which for new structures at least meets the Class 5 standards set forth in Federal Specification AA-D-6008 of the Federal Specifications and Standards cited in 41 CFR 101.
67. TOP SECRET. The classification level applied to information whose unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security. (The highest classification level.)
68. TRANSPORTATION SAFEGUARDS SYSTEM. The program, managed and operated by the Manager, Albuquerque Operations Office, under the programmatic direction of the Deputy Assistant Secretary for Military Application (DP-20), which has the administrative and courier personnel, special transport and escort vehicles, and nationwide high frequency communications system, SECOM, required to carry out the total responsibility for the safe secure domestic transportation of all Departmental-owned or -controlled nuclear explosives and Category I quantities of SNM and Plutonium-238 in quantities of 5 grams or greater.
69. VAULT TYPE ROOM. A DOE-approved room having combination-locked door(s) and protected by a Departmental-approved intrusion alarm system activated by any penetration of walls, floor, ceiling, or openings, or by motion within the room.
70. VITAL AREA. A security area for the protection of vital equipment.
71. VITAL EQUIPMENT. Equipment, systems, or components whose failure or destruction would cause unacceptable interruption to a national security program or harm to the health and safety of the public.
72. WASTE. A term applied to any source or SNM which is no longer useful and uneconomical or infeasible to recover, including that which has become radioactive by any means to the extent that the material itself exhibits radioactivity of such a level that it must be handled and disposed of by special methods in order to protect the general public.
73. WEAPON DATA. Classified information, including Restricted Data or Formerly Restricted Data, concerning the design, manufacture, or utilization, including theory, development, storage, characteristics, performance, and effects, of atomic weapons or components thereof, including such information incorporated in or relating to nuclear explosive devices.

TABLE OF CONTENTS

CHAPTER I - PHYSICAL PROTECTION PLANNING

Page

1. Threat Considerations.....	I-1
2. Program Planning Requirements and Documentation.....	I-1
3. Program Planning Considerations.....	I-2
4. Exceptions.....	I-2
5. Classified Special Nuclear Material.....	I-3

CHAPTER II - ACCESS CONTROL AND SECURITY AREAS

1. Basic Considerations.....	II-1
2. Security Areas.....	II-1
3. Requirements for Security Areas.....	II-2
4. Secure Communications Centers.....	II-6
5. Alarm System Central Stations.....	II-7
6. Automatic Data Processing Centers and Remote Interrogation Points Processing Classified Information.....	II-7
7. Sensitive Compartmented Information Facilities	II-8
8. Physical Barriers.....	II-8
9. Personnel Identification System.....	II-12
10. Personnel and Vehicular Access Controls.....	II-16
11. Photocopy Machine Control.....	II-16
12. Examination of Handcarried Items.....	II-16
13. Prevention of the Use of Surreptitious Listening Devices.....	II-17
14. Classified Conferences.....	II-17
15. Equipment Emitting Electromagnetic Emanations.....	II-18
16. Soundproofing of Walls.....	II-18

CHAPTER III - PROTECTIVE FORCE PERSONNEL

1. Medical and Physical Fitness Qualification Standards.....	III-1
2. Security Inspector Force.....	III-1
3. Guards.....	III-9
4. Communications for Protective Personnel.....	III-10
5. Security Inspector Post Standards.....	III-10
6. Limited Arrest Authority and Use of Force by Protective Force Officers.....	III-11

CHAPTER IV - INTRUSION DETECTION

1. Interior Protection Alarms.....	IV-1
2. Protective Lighting.....	IV-5

CHAPTER V - PHYSICAL PROTECTION OF CLASSIFIED MATTER

1. Physical Protection of Classified Matter in Use.....	V-1
2. Protection of Classified Matter in Storage.....	V-1
3. Protection of Classified Matter in Transit.....	V-7

CHAPTER VI - PHYSICAL PROTECTION OF SPECIAL NUCLEAR MATERIAL

1. Basic Considerations.....	VI-1
2. Special Conditions.....	VI-2
3. General Requirements.....	VI-3
4. Protection of Category I Quantities of Special Nuclear Material - In Use or Storage.....	VI-3
5. Protection of Category I Quantities of Special Nuclear Material - In Transit.....	VI-4
6. Protection of Category II Quantities of Special Nuclear Material - In Use or Storage.....	VI-7
7. Protection of Category II Quantities of Special Nuclear Material - In Transit.....	VI-8
8. Protection of Category III Quantities of Special Nuclear Material - In Use or Storage.....	VI-10
9. Protection of Category III Quantities of Special Nuclear Material - In Transit.....	VI-11
ATTACHMENT VI-1 - Physical Protection Categorization of Nuclear Material.....	VI-13

CHAPTER VII - PHYSICAL PROTECTION OF DEPARTMENTAL PROPERTY AND FACILITIES

1. Basic Considerations.....	VII-1
2. Standards and Requirements.....	VII-1

CHAPTER VIII - TRESPASSING ON DEPARTMENTAL PROPERTY

1. Statutory Provisions.....	VIII-1
2. Criteria.....	VIII-1
3. Proposals.....	VIII-1
4. Posting Requirements.....	VIII-2
5. Notification to the Federal Bureau of Investigation.....	VIII-2
6. Violations.....	VIII-2
ATTACHMENT VIII-1 - Example of a "No Trespassing" Sign for a Department of Energy Facility.....	VIII-3

CHAPTER IX - PHYSICAL PROTECTION OF DEPARTMENTAL NUCLEAR REACTORS

1. Policy and Objectives.....	IX-1
2. General.....	IX-1
3. Procedures and Requirements.....	IX-1

CHAPTER I

PHYSICAL PROTECTION PLANNING

1. THREAT CONSIDERATIONS.

- a. Planning for physical protection and access controls must account for the potential of an insider threat as detailed in specific guidance issued periodically by DP-1. Additionally, threats to security interests may be posed by individuals who do not possess authority for access to those interests. Individuals without access may act in concert with individuals who possess access authorizations.
- b. Acts which should be protected against include theft, sabotage, facility seizure, and other criminal acts.
- c. Classified threat guidance is developed by the Office of Safeguards and Security (DP-34) and is issued as policy by the Assistant Secretary for Defense Programs. This threat guidance may be modified periodically and updated as conditions dictate.

2. PROGRAM PLANNING REQUIREMENTS AND DOCUMENTATION.

- a. Baseline Compliance. This Order serves as the baseline compliance requirements document for the physical protection of new and existing facilities. As such, the requirements of this Order are minimum standards.
- b. Performance Requirements. Where applicable, additional requirements for the adequate performance of safeguards and security systems are contained in the classified threat guidance issued by DP-1.
- c. Program Documentation. There are two basic program documentation requirements. These are:
 - (1) Locally developed and approved site-specific safeguards and security plans, which may be transmitted to DP-34 or other organizations for information but not approval.
 - (2) Operations Office Master Safeguards and Security Plans. These plans are developed by the Heads of Field Organizations, and submitted to DP-34 for review and concurrence.

3. PROGRAM PLANNING CONSIDERATIONS. The basic considerations and factors pertinent to the type and degree of physical protection provided for security interests are:
 - a. Relative importance of the facility to the overall Departmental program, considering such matters as the availability of alternate facilities which could be used in an emergency;
 - b. Level of classification of Departmental interests;
 - c. Vulnerability of SNM, classified matter, vital facilities, equipment, or material to acts of arson, civil disorders, espionage, riots, sabotage, facility seizure, theft, terrorism, or vandalism;
 - d. State of emergency preparedness and the potential effects on the health and safety of the public and of Department and Departmental contractor employees;
 - e. Quantities, chemical and physical form, isotopic composition, containment, ease of separability, radioactivity, portability, chemical purity, ease of concealment, and accessibility of SNM;
 - f. Location, size, and arrangement of the facility and number of personnel involved;
 - g. Extent of need for integrating security measures with facility operations;
 - h. Probable duration of operations, and probability of expansion, curtailment, or other significant change in operations;
 - i. Need for compartmentalization of classified matter and activities;
 - j. Relative efficiency and economy of alternate methods of protection, such as deployment of protective forces or use of escorts to assure the most efficient use of manpower consistent with security requirements.
4. EXCEPTIONS. When it is impractical or not cost effective to meet a specific requirement of this Order, then alternate means of providing adequate protection may be proposed. Such exceptions to the Order should be developed by the Heads of Field Elements. There are three categories of exceptions.
 - a. Affecting the security of Category II (or greater) quantities of SNM and/or materials, facilities, or operations covered by the classified threat guidance issued by DP-1. These exceptions should

be developed by the Heads of Field Elements, and submitted in writing to DP-34 for review and consultation prior to implementation. Written records of such exceptions should be included in the appropriate site-specific safeguards and security plan(s).

- b. Affecting the security of less than Category II quantities of SNM and/or materials, facilities or operations not covered by the classified threat guidance issued by DP-1. These exceptions should be developed and approved by the Heads of Field Elements. Written records of such exceptions should be included in the appropriate site-specific safeguards and security plan(s).
 - c. Exceptions to the provisions of this Order, as provided in this section, shall be submitted in writing to the reviewing official within 12 months of the effective date of this Order.
5. CLASSIFIED SPECIAL NUCLEAR MATERIAL. When SNM is classified because of its configuration or content, or is part of a classified item, it shall receive, as a minimum, the physical protection required by the Order for the category of SNM involved, or that required by this Order for the assigned classification, whichever is greater.

CHAPTER II

ACCESS CONTROL AND SECURITY AREAS

1. BASIC CONSIDERATIONS.

- a. Controls shall be established to prevent unauthorized access to security areas or removal of security interests.
- b. Access to security areas or security interests shall be limited to persons who possess appropriate access authorization or certification, and who require such access in the performance of their official duties, on a need-to-know basis.
- c. Persons without appropriate access authorization or certification for the area visited shall be escorted by an appropriately cleared person at all times within security areas in which unsecured security interests are located. When there are also local restrictions on access due to operating, technical, or compartmentalization considerations, only persons conversant with such restrictions shall serve as escorts for visitors.

2. SECURITY AREAS.

- a. A security area denotes a physically defined space established to protect a security interest and subject to physical protection and access controls.
- b. Security areas are established when the nature, size, revealing characteristics, sensitivity, or importance of the security interests is such that access to them cannot otherwise be effectively controlled.
- c. The type of security area established depends on the nature of the security interests to be protected, with the following types required for the protection of the listed security interests:
 - (1) Property Protection Area for protection of Departmental property, located at property protection facilities (see Chapter VII).
 - (2) Limited Area for protection of classified matter where guards, security inspectors, or other internal controls can prevent access by unauthorized persons to classified matter.
 - (3) Exclusion Area for protection of classified matter where mere access to the area would result in access to classified matter.

- (4) Protected Area for protection of irradiated or unirradiated Category I and II special nuclear material (see Chapter VI).
 - (5) Material Access Area within a protected area for protection of Category I special nuclear material (see Chapter VI).
 - (6) Vital Area within a protected area for protection of vital equipment.
- d. Offices of consultants or other individuals, small laboratories, or other facilities with limited scope and volume of work normally do not require establishment of security areas. However, adequate security must be in place to preclude unauthorized access.

3. REQUIREMENTS FOR SECURITY AREAS.

a. Property Protection Area shall include:

- (1) Clearly defined perimeter barriers;
- (2) Personnel and vehicle access controls;
- (3) Personnel identification system;
- (4) Establishment and maintenance of a visitors' log;
- (5) Means to provide timely detection of intrusion by use of alarm systems or other means such as random patrols or visual surveillance; and
- (6) Signs prohibiting trespassing posted around the perimeter and at the entrances, and reward signs and signs prohibiting the introduction of contraband articles and authorizing inspections/ searches of vehicles, packages, or persons either entering or exiting posted at all entrances.

b. Limited Area shall include:

- (1) Clearly defined perimeter barriers;
- (2) Personnel and vehicle access controls;
- (3) Personnel identification system;
- (4) Establishment and maintenance of visitors' log;
- (5) Means to provide timely detection of intrusion by use of alarm systems or other means such as random patrols or visual surveillance.

- (6) Signs prohibiting trespassing posted around the perimeter and at the entrances, and reward signs and signs prohibiting the introduction of contraband articles and authorizing inspections/searches of vehicles, packages, or persons either entering or exiting posted at all entrances;
 - (7) Measures to prevent unauthorized visual or aural access to classified matter, including soundproofing of floors, walls and ceilings, soundbaffling of air ducts, and measures to detect surreptitious listening devices and to prevent their use (refer to DOE 5636.3);
 - (8) Entrance inspections/searches, when conducted, shall be accomplished to prevent the unauthorized introduction of explosives, cameras, electronic recording or transmitting equipment, or other prohibited articles. All vehicles and visitor handcarried items (e.g., briefcases, lunchpails, and so forth) shall be subject to inspection/search. Articles handcarried by employees may be inspected/searched on a random basis;
 - (9) Exit inspections/searches, when conducted, shall be accomplished to prevent the unauthorized removal of classified matter or Government property. All vehicles and visitor handcarried items (e.g., briefcases, lunchpails, and so forth) shall be subject to inspection/search. Articles handcarried by employees may be inspected/searched on a random basis;
 - (10) Measures for the protection of data processing; and
 - (11) All security-related subsystems and components maintained in readily operable condition shall have a regularly applied test and maintenance program to assure an effective operable system.
- c. Exclusion Area. In addition to the requirements as listed for a limited area, an exclusion area requires that all individuals afforded access must have an access authorization consistent with the highest classification of matter to which they would have access by sole virtue of their presence in the area.
- d. Protected Area shall include:
- (1) Clearly defined perimeter barriers;
 - (2) Personnel and vehicle access controls administered by security inspectors;
 - (3) Personnel identification system;

- (4) A properly maintained visitors' log;
- (5) Continuous intrusion alarm system sufficient to provide timely detection of intrusion, or, for temporary situations until an alarm system can be installed, the area shall be occupied by at least two security inspectors who can visually detect intrusion on a 24-hour basis and who have at least two means of communication to a point from which response forces can be dispatched. During times when the perimeter alarm or equivalent is not in operation, the perimeter shall be patrolled (on a random basis) by security inspectors at intervals not exceeding an hour;
- (6) Protective lighting sufficient to provide 24-hour visual surveillance assessment capability;
- (7) Posting of facilities and property against trespassing; appropriate reward signs; signs shall be posted at all entrances prohibiting the introduction of prohibited articles and authorizing inspections/searches of personnel, handcarried items, and vehicles entering or leaving;
- (8) A hardened protective force communications center shall be established and shall have periodically tested radio, if available, and telephone channels of communication with local law enforcement agencies. There also shall be an emergency alternate communications capability from a secondary station for use in the event the primary station is compromised. Radio communications equipment shall remain operable in the event of a loss of primary electrical power;
- (9) Security inspector posts, both mobile and fixed, shall be equipped with duress systems;
- (10) Private use vehicles shall be excluded. Government-owned or Government-leased vehicles shall be admitted only when on official business and when operated by properly cleared and authorized drivers or who are under escort by properly cleared and authorized personnel. Service and delivery vehicles shall be admitted to protected areas only when on authorized business and when driven or under escort by properly cleared and authorized personnel. Access by such vehicles shall be kept to a minimum consistent with operational requirements. Service and delivery vehicles shall not be admitted strictly for the convenience of the service or delivery personnel;
- (11) Inspection/search of personnel, handcarried items, and vehicles shall be provided as follows:

- (a) Entrance inspections/searches of all personnel and of all vehicles and handcarried items shall be conducted to prevent the introduction of explosives, weapons, or other prohibited articles. The inspection/search on entering may be made with Department-approved detection equipment designed to assure that explosives, weapons, or other prohibited articles are not introduced.
 - (b) Albuquerque Operations Office/Transportation Safeguards Division couriers and vehicles shall be exempt from these requirements when on official business.
 - (c) Exit inspections/searches shall be accomplished to prevent the unauthorized removal of SNM, classified matter, or other Government property. All visitor handcarried items (e.g., briefcases, lunchpails, and so forth) and all service and delivery vehicles shall be inspected/searched. Articles handcarried by employees and Government-owned or Government-leased vehicles may be inspected/searched on a random basis, so long as at least 5 percent of all such items are searched.
- (12) All detection/alarm devices, including transmission lines to annunciators, shall be failure and tamper-indicating in both the access and service modes. Such devices shall be connected to monitor/display panels in the hardened security force communications center. An alternative alarm annunciation point (or a comparable alternate capability) shall be provided in a location which is continuously manned by cleared personnel and which provides a second indication of an alarm such that a response can be initiated in the event the primary station is compromised; and
- (13) All security-related subsystems and components shall be maintained in readily operable condition, and shall have a test, maintenance, and quality assurance program to ensure an effective operable condition.

e. Material Access Area.

- (1) Material access areas are contained within protected areas.
- (2) Access to material access areas shall be controlled to limit entry to appropriately cleared or escorted individuals who require admittance to perform their official duties.
- (3) Rooms, buildings, or portions of a building within a material access area containing unattended Category I quantities of in-process SNM shall be equipped with Department-approved intrusion alarm systems, or other equally effective means of detection.

- (4) Security inspector response time to alarms shall not be more than 5 minutes. Alternately, response time shall be less than the delay time that can be demonstrated from alarm activation until intruders could complete their adverse actions.
- (5) Records shall be maintained of all persons who are admitted to material access areas who are not directly employed in operations involving access to, or use, processing, storage, accountability, or protection of SNM and of all persons who enter such areas during nonoperating hours.
- (6) Exit inspections/searches of all personnel, vehicles, and hand-carried items including packages, briefcases, and lunchpails shall be conducted to prevent unauthorized removal of special nuclear material. Personnel inspections/searches may be accomplished through the use of SNM portal monitors and metal detectors.
- (7) SNM shall be in storage or under material surveillance procedures.

f. Vital Area.

- (1) Vital areas are contained within protected areas.
- (2) Access to vital areas shall be controlled to limit entry to appropriately cleared or escorted individuals who require admittance to perform their official duties.
- (3) Unoccupied rooms or buildings (or a portion of a building) within a vital area containing vital equipment shall be equipped with a Department-approved intrusion alarm system, or other equally effective means of detection.
- (4) Security inspector response time to alarms shall not be more than 5 minutes. Alternately, response time shall be less than the delay time that can be demonstrated from alarm activation until intruders could complete their adverse actions.

4. SECURE COMMUNICATIONS CENTERS.

- a. Communications centers handling classified messages shall be located within, or established as, security areas.
- b. When contained within a security area, a communications center requires separate access controls and barriers to restrict admittance to persons who are employed therein or who require access in the performance of official duties.

- c. Access authorizations consistent with the highest level of classified information handled shall be required for all persons assigned to or having any unescorted access to secure communications centers. A list of persons authorized such access shall be posted at the entrance to the center and a record of all visitors entering the facility shall be maintained.
 - d. The Department's security representatives shall conduct security surveys of secure communications centers to assure the adequacy of physical security, access controls, and access authorization requirements. Findings resulting from these security surveys shall be incorporated as part of the regular security survey report.
 - e. The Office of Computer Services and Telecommunications Management (MA-25) administers the classified telecommunications program in coordination with DP-34, whose responsibilities and authorities for the physical protection of classified telecommunications information are set forth in DOE 5300.3A and the DOE procedural guide titled "COMSEC Procedural Guide," of 2-28-83.
5. ALARM SYSTEM CENTRAL STATIONS. The Headquarters locations of a central station alarm system shall be protected as follows:
- a. Commercial central alarm stations should be Underwriter Laboratories listed Grade AA installations. The responsible field element should assure that the selection of central station alarm systems equipment to be used is made to the extent possible on available test data.
 - b. Facility central stations shall be located within, or established as, security areas, and constantly attended even when contained within a security area. The central stations also require separate access controls and barriers to restrict admittance to persons employed therein or requiring access in the performance of official duties on a need-to-know basis.
 - c. Local law enforcement agency central stations are usually constantly attended. If response by local law enforcement agencies to an alarm device is required for facility approval, the connection to the local law enforcement agency central station should meet the specification contained in UL-Class A of UL-365, "Police Station Connected Burglar Alarm Systems and Units."
6. AUTOMATIC DATA PROCESSING CENTERS AND REMOTE INTERROGATION POINTS PROCESSING CLASSIFIED INFORMATION.
- a. The security afforded automatic data processing (ADP) centers and remote interrogation points shall conform to the policy as set forth in DOE 5636.2, DOE 5636.4, and DOE 1360.2.

- b. ADP centers and remote interrogation points used for classified information shall be located within or established as security areas.
 - c. ADP centers and remote interrogation points used to process classified information shall require separate access controls and barriers to assure access to classified information is limited to those persons requiring access in the performance of official duties and within the need-to-know parameters.
 - d. Where transmissions of classified data outside security areas are involved, National Security Agency-approved encryption shall be used or the signal lines shall be installed in accordance with DOE 5300.4A.
 - e. Access authorizations consistent with the highest level of classified information processed shall be required for all persons who are assigned to or have unescorted access to ADP centers and remote interrogation points which process classified data. A list of all persons authorized unescorted access to the ADP facility shall be maintained at the entrance to the facility. Additionally, a record of all visitors entering such areas shall be maintained.
 - f. The Department's security representatives shall conduct security surveys of ADP centers and remote interrogation points which process classified data to assure the adequacy of computer security. Findings resulting from these surveys shall be incorporated as part of the regular security survey report.
7. SENSITIVE COMPARTMENTED INFORMATION FACILITIES. During the regular security survey, security representatives shall also conduct surveys of sensitive compartmented information facilities. These surveys will cover only the physical attributes of security. The findings resulting from these surveys shall be incorporated as part of the regular security survey report.
8. PHYSICAL BARRIERS.
- a. Physical barriers such as fences, walls, and doors shall be used to deny or impede unauthorized access to security areas. They facilitate effective use of protective force personnel and direct the flow of personnel and vehicular traffic through designated portals.
 - b. Permanent barriers shall be used to enclose security areas except during construction or transient activities, when temporary barriers may be erected.

- c. The following standards apply to fences, walls, floors, ceilings, doors, windows, locks, and unattended openings:

(1) Permanent Fences.

- (a) Utilized for the protection of security areas shall consist of No. 11 American Wire Gauge, or heavier, steel wire fabric woven or tied so that openings cannot be easily expanded or footholds readily gained for scaling. Fences shall be topped by three or more strands of barbed wire on brackets, angled outward where possible, or by coiled barbed wire (concertina) or barbed ribbon. Fencing fabric shall extend to within 2 inches of firm ground or below the surface if the soil is unstable or subject to erosion by wind or water. Overall fence fabric height shall not be less than 7 feet exclusive of outriggers and barbed wire or barbed ribbon. Fencing fabric shall be mounted on steel posts set in concrete with additional bracing as necessary at corners and gate openings. Posts, bracing, and other structural members shall be located inside the area.
- (b) Shall be installed not more than 500 feet, or less than 20 feet, from the building or matter under protection. Where these distances cannot be observed because of property lines, building locations, health and safety or other site-specific considerations, supplementary protective measures shall be provided, such as greater height of fences, parallel fence, or more frequent protective force patrols. Fence lines shall be kept clear of vegetation, trash, equipment, and other objects which could impede observation. Where practicable, at least 20 feet of clearance shall be maintained between fence lines and adjacent areas which could conceal potential intruders.

- (2) Temporary Fences may be of any height and material which will effectively impede access to the area.

(3) Walls.

- (a) Openings in walls must be covered by steel wire mesh (see subparagraph (7) below).
- (b) Where used, wire mesh shall be 2-inch square or smaller mesh of No. 11 American Wire Gauge or heavier steel wire or expanded metal.
- (c) Heavy-duty builders' hardware shall be used, and all screws, nuts, bolts, hasps, clamps, bars, wire mesh, hinges, and hinge pins shall be fastened securely to preclude surreptitious removal and assure visual evidence

of tampering. Hardware accessible from outside the area shall be peened, brazed, or spot welded to preclude removal or be otherwise secured by hardware that is inaccessible to unauthorized tampering (e.g., nonremovable hinge pins).

- (d) Walls to security areas shall be at least 8-feet high and be constructed of solid building materials (e.g., plaster, gypsum, wallboard, metal panels, wood, and so forth) or other opaque or translucent materials offering substantial resistance to and evidence of unauthorized entry into the area, of shatter-resistant, laminated glass of 9/32-inch minimum thickness if visual access can be prevented effectively by the use of drapes, blinds, or other means; or if steel wire mesh is used, a securely fastened overlap molding is necessary. If insert-type panels are used, removal of the panels from outside the area shall not be possible without visual evidence of tampering. Walls should extend from the floor to the structural ceiling when they constitute exterior barriers of areas in which classified information is discussed. When walls do not extend to the ceilings of storage rooms or areas, the gaps should be closed with mesh or material equivalent in resistance to the walls.

(4) Doors.

- (a) Openings in doors must be covered by steel wire mesh (see subparagraph (7) below).
- (b) Doors shall offer substantial resistance to unauthorized entry but need not be more resistant to penetration than adjoining walls, ceiling, and floors. If visual access is not a factor, doors with glass panels may be used; however, they shall meet the specifications set forth in paragraph 8c(4) or shall be equipped with wire mesh fastened securely to the door, preferably on the inside. When visual access is a factor, a sight baffle shall be used when a door is open. When doors are used in pairs, an overlap molding is required where the doors meet. Door louvers or baffle plates, when used, require reinforcement. Door jams shall be reinforced when necessary to make it more difficult to open by use of a wedge, jimmy, or similar tool.

(5) Ceilings and Floors.

- (a) Openings in ceilings and floors must be covered by steel wire mesh (see subparagraph (7) below).

- (b) Ceilings and floors shall offer substantial resistance to unauthorized entry. Steel wire mesh may be used if visual or aural access is not a factor.
- (6) Windows. Where primary reliance is placed on windows as physical barriers, they shall be constructed of shatter-resistant, laminated glass panes of 9/32-inch minimum thickness or other material providing an equivalent degree of resistance, and installed in fixed (e.g., nonopenable) frames so that the panes are not removable from outside the area being protected. The frames must be securely anchored in the walls, and windows should lock from the inside. Swingout steel sash (industrial type) is acceptable for window installation provided the windows can be securely locked or are permanently sealed shut.
- (7) Unattended Openings. Unattended openings in barriers which are more than 96 square inches in area and over 6 inches in smallest dimension shall be alarmed or equipped with steel wire mesh or 1/2-inch steel bars on not more than 6-inch centers, with securely anchored or fastened steel cross bars to prevent spreading. This provision applies when an opening is located less than:
 - (a) Eighteen feet above uncontrolled ground, roofs, or ledges.
 - (b) Fourteen feet diagonally or directly opposite windows, fire escapes, roofs, or other openings in uncontrolled buildings.
 - (c) Six feet from uncontrolled openings in the same barrier.
- (8) Locks.
 - (a) A combination lock shall meet Underwriter Laboratories' Standard No. 768, Group I-R.
 - (b) A combination padlock shall meet FF-P-110 of the Federal Specifications and Standards cited in 41 CFR Chapter 101.
 - (c) A key padlock shall meet military specification MIL-P-43951 or FF-P-001480.
 - (d) A key lockset shall meet American National Standards Institute, Inc., standards ANSI A156.2.
 - (e) Combinations of locks or padlocks on repositories containing classified matter shall be known only to those authorized access to the matter and shall be changed when repositories are placed in use, whenever a person knowing the combination is no longer

authorized access to the matter the combination protects, when the combination may have been compromised, or at least once every year.

- (f) Records of combinations shall be classified no lower than the highest classification of the matter stored in the repository but do not require authentication when classified Top Secret.
- (g) Panic locks used on emergency exit doors in security area perimeters shall be operable only from the inside and shall be equipped with at least a loud local alarm. Door locks and latches shall comply with National Fire, Protection Association (NFPA) Code 101.
- (h) Lock bars shall be 1-1/4 inch by 3/16 inch or equivalent in cross section and constructed of material hardened to Rockwell C59 to C63 standards.
- (i) Hasps and yokes on repositories containing classified matter shall be constructed of material hardened to Rockwell C59 to C63 standards and at least 1/4 inch in diameter or equivalent cross section and secured to the repositories by welding or riveting.
- (j) Keys to locks or padlocks on containers holding classified matter, SNM, or used to secure gates or doors in security area perimeters shall be issued only to persons authorized access to the matter or to the area. Key locks should be resistant to picking and jimmying and combination locks should be resistant to manipulation. Padlocks should be of sturdy construction and resistant to opening by picking, rapping, forcing, or the use of shims or similar techniques. A system of accountability and positive controls for keys and combinations should be in place. When a key is unaccounted for, the lock(s) which it opens should be replaced immediately. Combinations should be changed when a person having access thereto is terminated or permanently assigned outside the function involved.

9. PERSONNEL IDENTIFICATION SYSTEM.

- a. A Security Badge or Pass System shall be used to assure that only authorized personnel enter and leave a security area and to indicate limitations placed upon access to classified matter and information.

- (1) A badge or pass system shall be used to control access to a security area in which 30 or more persons are employed.
 - (2) Personal recognition may be used in lieu of a badge or pass system to control access to a security area in which fewer than 30 persons are employed per shift.
 - (3) A badge or pass system shall be used for personnel access controls as set forth in this Order.
- b. Employees and Visitors within a security area shall wear conspicuously on the upper front portion of the body the badge or pass required for entrance into the area unless prohibited by health or safety regulations.
- c. DOE Employee Identification Badge or Pass (DOE F 5631.19).
- (1) Employee badges or passes shall be issued only to Departmental employees and may be accepted as authority for admission to all Departmental facilities. The term "Departmental employee" encompasses members of the Armed Forces assigned to and performing duties under the direction and control of the Department, designated representatives of the Military Liaison Committee, and employees of the Department.
 - (2) Inserts for these badges or passes are procured and controlled by DP-34 and distributed to each field element for issuance.
- d. Types of Contractor and Subcontractor Badges or Passes.
- (1) Permanent Employees.
 - (a) Badges or passes for permanent employees shall contain on the face or front the name and location of the issuing office, the contractor or subcontractor, and the name and clear photograph of the employee. A prominently displayed serial number shall also appear on the badge or pass.
 - (b) Badge or pass information may also include the personal description and the signature of the holder, and the signature (or facsimile) of the official authorizing its issuance. Coding indicating categories of information or areas within the facility to which the bearer is authorized access, or the degree of access authorization, may also be included.

- (2) Visitors. Badges or passes for visitors shall bear, as a minimum, the following data:
 - (a) For escorted visitors: a serial number and indication on the face of the badge or pass that escort is required. If the visitor is an alien, the badge or pass should so indicate.
 - (b) For unescorted visitors: the name of the visitor, type of access authorization; security areas the visitor is permitted to enter, if appropriate; and expiration date, except that badges not removed from the facility need show only a serial number and type of access authorization, security clearance, or areas to which the visitor is permitted or allowed unescorted access.
- (3) Temporary Employees shall be issued badges or passes conforming to requirements for permanent employees or unescorted visitors.
- (4) Construction Workers and others whose work is so located or whose movements are so controlled that they do not have access to security areas or to classified matter may be issued badges which contain only the name of the employer or issuing authority and a number conspicuously displayed on the face thereof.

e. Badge and Pass Specifications.

- (1) Badges and passes for permanent employees are subject to the following specifications:
 - (a) Dimensions of the photograph, exclusive of the name, shall be not less than 1-1/2 inches long by 1-1/4 inches wide, and the facial image shall be as large as practicable within these limits.
 - (b) The face of the insert or the bonding material shall contain an ink or dye noticeably affected by the heat, erasure, or solvent necessary to relamine, remake, or alter the badge or pass (fluorescent inks or dyes, magnetized matter, water marks, superimposed cross threads or wire, or other material designed to prevent fraudulent use may be used).
 - (c) Inserts shall be laminated between sheets of transparent plastic material in such a manner that the plastic becomes securely bonded together and completely covers the insert.

- (d) All badge inserts shall be serially numbered and a strict accountability or control of plates and inserts, including those scrapped or spoiled, shall be maintained.
- (2) Badges and passes for permanent employees may be manufactured by processes other than those set forth in paragraph 9e(1) above, provided the degree of tamper resistance is equivalent to or greater than that specified.
- (3) Badges for construction workers or other persons not requiring access to security areas may be of any suitable substantial material.
- f. Disposition Records shall be maintained by the facility showing the disposition of all badges and passes. Such records shall include date of issuance, name of holder, type of access authorization, and, if applicable, the categories of information and the areas within the facility to which access is authorized.
- g. A Record of Lost Badges and Passes shall be kept and personnel controlling access to security areas shall be notified in order to prevent their misuse. The loss or recovery of an employee identification badge or pass shall be reported immediately to DP-34, who in turn shall notify all concerned field elements which shall make appropriate notification to contractors, subcontractors, and other organizations under their jurisdiction.
- h. Stocks of Inserts and Unissued Badges and Passes shall be stored in a manner assuring their protection against loss, theft, or unauthorized use. As a minimum, they shall be stored in a manner approved for the storage of Confidential matter.
- i. Badges and Passes of Terminating Employees shall be recovered. Badges and passes issued to visitors will be recovered at the conclusion of each visit.
- j. Reissuance of Badges and Passes.
 - (1) Security badges and passes issued to permanent employees shall be replaced by a new issuance having a different background design or color, with new photographs, when 5 percent of the badges currently in use have been lost, or at least every 5 years.
 - (2) If a significant change in facial appearance takes place, a badge or pass with a new photograph shall be requested and issued.

10. PERSONNEL AND VEHICULAR ACCESS CONTROLS.

- a. Verification of the identity of persons authorized access to a security area shall be accomplished at the entrance by the protective force, receptionist, or other person assigned for that purpose, except that remote identification by television may be used, provided that positive identification is assured. Also, an unattended mechanical or electrical admittance system may be used at an inner security area (e.g., within a larger security area).
- b. Entrances to and exits from security areas shall be equipped with doors, gates, rails, or other movable barriers which will direct and control the movement of personnel or vehicles through designated portals.
- c. A visitor log shall be maintained to reflect the name, signature, organization, and citizenship of each uncleared visitor to a security area, persons visited, escort names and signatures, purpose of visit, and time in and out of the security area.
- d. A visitor without appropriate access authorization or certification shall be escorted at all times while within a security area by protective force personnel, the person being visited, or other employees assigned for that purpose.

11. PHOTOCOPY MACHINE CONTROL. Machines used for the reproduction of classified documents shall be located in security areas to the greatest extent possible commensurate with organizational capabilities. Internal procedures must be established to monitor the utilization of such equipment to protect against unauthorized use.12. EXAMINATION OF HANDCARRIED ITEMS.

- a. The following articles shall not, without proper authorization, be taken into security areas:
 - (1) Firearms, ammunition, explosives, or incendiary devices;
 - (2) Cameras, copying, or reproduction devices;
 - (3) Recording or transmitting devices;
 - (4) Alcohol, alcoholic beverages, or illegal drugs;
 - (5) Other items similar in effect or purpose to any of the above; or
 - (6) Any other items prohibited by law.

- b. As a condition of ingress to and egress from security areas, handcarried items may be subject to inspection/search.
- c. Notices setting forth the policy and requirements of this chapter shall be posted at each entrance to security areas.
- d. When inspection/search of a package, box, briefcase, or similar article discloses a prohibited item and there is no reasonable explanation for its presence, or there is other indication of possible violation of Federal law, the matter shall be reported immediately in accordance with the provisions of DOE 5633.1.

13. PREVENTION OF THE USE OF SURREPTITIOUS LISTENING DEVICES.

- a. Offices or rooms in security areas where Secret or Top Secret information is discussed or processed (by automatic data processors, private telephone systems, and so forth) shall be inspected on a recurring basis under the cognizance of DOE 5636.3.
- b. Buildings under construction or renovation shall be examined, when feasible, to assure that listening devices are not concealed.
- c. Conference rooms outside security areas shall be inspected prior to any conference involving classified information. In addition, an examination shall be made immediately prior to each session, unless the room is kept under continuous control between conference sessions. Permanently installed public address systems shall be subject to the same examination, removal, or deactivation as telephone equipment. When preparing the required notification concerning classified conferences, Classification Guide, CG-TSCM-1, should be consulted.
- d. Inspections of telephone equipment and public address systems shall be conducted by appropriately access-authorized and qualified personnel of the Department, contractors, or telephone companies.
- e. Telephones or public address systems in conference rooms or offices in which classified discussions at the Secret or Top Secret level occur should be equipped with plug and jacks or other disconnecting devices to allow for disconnection during classified discussions.

14. CLASSIFIED CONFERENCES.

- a. Conferences involving classified information shall be held within security areas, except as provided below.
- b. Conferences involving classified information may be held outside security areas only when it is impracticable to hold them within such areas, when adequate protection can be provided, and when authorization has been granted by the Heads of Field Elements or, in the case of Headquarters, by DP-34.

- c. A request to hold a classified conference outside an existing security area shall be submitted to the responsible Heads of Field Elements, or in the case of Headquarters, to DP-34, at least 15 days prior to the date of conference and shall contain the following information as appropriate:

- (1) Purpose and nature of the conference;
- (2) Approximate number of participants;
- (3) Physical location of the proposed conference;
- (4) Classification and information categories involved;
- (5) Justification for holding the conference outside security areas;
- (6) Description of existing security restrictions bearing on classified information or matter involved;
- (7) Name(s) of person(s) responsible for security of the conference;
- (8) Description of the conference area and security precautions to be taken; and
- (9) Information concerning any permanently installed telephones or sound amplifying equipment or other known situations of possible concern to the security of the conference.

15. EQUIPMENT EMITTING ELECTROMAGNETIC EMANATIONS. Data processing, amplifying, telecommunications, and other systems which emit electromagnetic emanations, and communications lines to remote interrogation points used to process classified data processing information, shall be protected against compromise of such data in accordance with the standards set forth in DOE 5636.2, DOE 5300.2A, and DOE 5300.4A.

16. SOUNDPROOFING OF WALLS. Walls, ceilings, and doors of offices or rooms constituting security area perimeters where Secret or Top Secret information is discussed on a recurring or routine basis shall be constructed of materials of low sound conductivity, or shall otherwise be soundproofed in accordance with DOE 5636.3, so as to prevent a person outside the room with reasonable access to the wall from overhearing a conversation at normal voice level within the room without the use of hearing instruments or equipment.

CHAPTER III
PROTECTIVE FORCE PERSONNEL

1. MEDICAL AND PHYSICAL FITNESS QUALIFICATION STANDARDS. Incumbent and applicant security inspectors and guards at Department-owned facilities are required to meet the applicable medical and physical fitness qualification standards contained in 10 CFR 1046, "Physical Protection of Security Interests."
2. SECURITY INSPECTOR FORCE.
 - a. When Required. A security inspector force is required at facilities which:
 - (1) Are Class A or Class B facilities, except those which are utilized solely as administrative areas;
 - (2) Contain nuclear weapons, nuclear test devices, complete nuclear assemblies, or significant quantities of special nuclear material (Category II or greater); or
 - (3) Contain security areas in which classified matter cannot be safeguarded adequately during working hours by employees or guards, or during nonworking hours by alarm protection or guard patrols.
 - b. Duties. Security inspectors shall perform the following duties:
 - (1) Enforce regulations concerning trespass, exclusion of prohibited articles, personnel identification, protection of classified matter, and special nuclear material;
 - (2) Observe and patrol designated perimeters, areas, and structures;
 - (3) Prevent persons or vehicles from gaining unauthorized access to security areas;
 - (4) Check repositories, rooms, or buildings containing classified matter during nonworking hours to determine that they are locked or otherwise in order;
 - (5) Perform escort duties;
 - (6) Respond to protective alarm signals or other indications of suspicious activity;

- (7) Act as necessary in the event of situations affecting the security of the facility, including fires, industrial accidents, internal disorders, and attempts to commit espionage, sabotage, or other criminal acts;
 - (8) Protect classified matter and Government property against unauthorized access, theft, or intentional damage; and
 - (9) Report to supervisors all incidents or unusual circumstances affecting or potentially affecting the security of the area at the time of occurrence or as soon thereafter as possible.
- c. Special Response Teams. Plans concerning emergency duties and the deployment of special response teams (facility deployment or, where feasible, through memorandums of understanding with local jurisdictions) shall be maintained at all Class A facilities. Special response teams shall assure adequate emergency response to events involving the attempted or actual sabotage of nuclear weapons, theft of nuclear weapons or test devices, Category I quantities of special nuclear materials, other selected strategic materials and associated facilities, labor disturbances, and other situations threatening the security of the facility that may be perpetrated by terrorists, criminals, psychotics, disgruntled employees, and antinuclear extremists.
- d. Training.
- (1) Prior to initial assignment to duty, each security inspector shall successfully complete a course of basic qualification consisting of a minimum of 80 hours of classroom and practical instruction. Qualification training courses shall include at least the following subjects:
 - (a) General orientation;
 - (b) Purposes and principles of the Department's system of security;
 - (c) Security as applied to the local installation;
 - (d) Organization and functions of the Department and Departmental contractor security inspector forces;
 - (e) Legal authority of the individual security inspector;
 - (f) Specific duties, including sufficient "break-in" training;
 - (g) Security inspector orders; general and specific;
 - (h) Discipline; obedience to orders;

- (i) Employee and public relations;
 - (j) Self-defense;
 - (k) Communications facilities and procedures;
 - (l) Elementary first aid and fire protection;
 - (m) Report writing;
 - (n) Riot control;
 - (o) Arrest authority;
 - (p) Weapons safety training;
 - (q) Safety and general training sufficient to provide knowledge of and protection from unique hazards of materials and operations;
 - (r) Operation and use of all security inspector post special and technical equipment such as metal, explosive, and SNM detectors, personnel identification systems, and night vision devices; and
 - (s) If assigned to protect nuclear weapons, nuclear test devices, or special nuclear materials, additional advanced and specialized training shall be provided as appropriate to assigned job functions.
- (2) Before a security inspector shall be considered adequately trained and assigned to fully independent duties, the security inspector shall be given either a written examination or appropriate appraisal to verify his or her readiness to carry out the responsibilities to be assigned. If written examinations are given, test papers shall be retained for examination during scheduled security surveys.
 - (3) Security inspectors shall be provided a minimum of 24 hours of refresher training annually. Subject material for refresher training should emphasize a review of duties, responsibilities, and procedures in which instruction is most urgently needed as determined by job performance and supervisor recommendations.
 - (4) Records shall be maintained of the nature of all training conducted and the names of the security inspectors so trained.
 - (5) In addition to individual training as specified above, each shift at each protected, vital, limited, and exclusion area shall conduct security response exercises. These exercises should be conducted at least monthly and should focus on preventing the successful completion of acts of facility or material seizure, theft, or sabotage.

- (6) Special response teams shall also train and exercise as teams in a variety of response situations. These should include hostage/barricade situations, force-on-force, surreptitious intrusion, airborne intrusion, building and/or area search and clear operations, and other scenarios derived from and germane to local conditions. Additionally, special response teams should exercise at least annually in coordination with the FBI and local law enforcement agencies who would respond to incidents at the team's facility.
- (7) Prior to duty assignment, each special response team member shall successfully complete classroom and practical instruction that shall include at least the following subjects:
 - (a) Adversary characteristics (objectives, equipment, communications);
 - (b) Hostage/barricade situations;
 - (c) Search and clear techniques;
 - (d) Rappelling;
 - (e) Special munitions (e.g., chemical);
 - (f) Special weapons (e.g., antiarmor);
 - (g) Day and night tactical movements;
 - (h) Special communications;
 - (i) Quick reaction shooting;
 - (j) Sniper situations;
 - (k) Explosive ordnance disposal familiarization; and
 - (l) Unconventional warfare

e. Firearms Qualification.

- (1) A security inspector shall not be authorized to carry a firearm until the responsible Head of the Field Element is assured, within the limitation of his or her normal administrative capabilities, that the individual who is to be armed is medically and physically fit as well as emotionally stable and has qualified in accordance with Departmental firearms standards. These requirements shall be applied to employees as set forth below.

- (2) All security inspectors shall qualify initially, and subsequently at least annually, using their assigned handgun and with the types of ammunition with which they are armed while on duty. For automatic and semiautomatic rifle and shotgun, they will qualify initially, and subsequently at least annually, using the type and barrel length of semiautomatic rifle and shotgun with the types of ammunition with which they are armed while on duty. Qualification shall be under both day and night conditions and shall be coupled with a review of the basic principles of firearms safety. An approved National Rifle Association or Federal law enforcement course such as the Federal Bureau of Investigation's Practical Pistol Course shall be used at the discretion of the Head of the Field Element. Initial establishment of requalification anniversaries for individual security inspectors on the various weapon courses of fire shall be at the discretion of the Head of the Field Element.
 - (3) Authority to carry a firearm shall be revoked if a security inspector fails to qualify annually on the approved courses of fire.
 - (4) DOE Form DP-614, "Firearms Qualification Record," shall be maintained for each security inspector who qualifies, or who attempts to qualify, under paragraph 2e(2) of this chapter. Each record shall be retained until the next scores are entered on a new record and placed in the security inspector's file. Current records shall be retained for 1 year after separation of a security inspector from security inspector duties. The security inspector force chief, or his or her supervisor, or the force's training officer shall be designated in writing as the individual authorized to certify the validity of the scores. Failure to certify a score prior to issuance of firearms authorization to a security inspector or submission of a false certification by the individual so designated shall be grounds for disciplinary action and/or legal action under title 18, section 1001, of the United States Code (U.S.C.).
- f. Authority to Carry Firearms. Section 161k of the Atomic Energy Act of 1954, as amended (42 U.S.C. 2201k), authorizes the appropriate arming of Department or Departmental contractor personnel while engaged in the protection of property of the United States. It also provides authority to make arrests without warrant. Each Departmental employee or Departmental contractor security inspector receiving this authorization shall be issued a laminated card containing the individual's photograph, signature, and actual or facsimile signature of the issuing Department or Departmental contractor official (if a facsimile signature is used on the card, a signed memorandum constituting the authorization shall be kept on file), date of issuance, and one of the following statements:

(1) For Departmental Employees:

"This is to certify that (individual's name) whose signature and picture appear hereon, has been granted the authority to perform all duties conferred upon United States Department of Energy Federal Officers under section 161k of the Atomic Energy Act of 1954, as amended (42 U.S.C. 2201k), including the authority to investigate, audit, require and receive information, to carry firearms while engaged in the performance of official duties, and to make arrests without a warrant while engaged in the performance of official duties as provided in 42 U.S.C. 2201k.

(2) For Departmental Contractor Employees:

"This is to certify that (individual's name), an employee of (name of company) whose signature and picture appear hereon, has been granted the authority under section 161k of the Atomic Energy Act of 1954, as amended (42 U.S.C. 2201k), to carry firearms and to make arrests without warrant while engaged in the performance of official duties as provided in 42 U.S.C. 2201k."

g. Equipment.

(1) Uniform. Security inspector personnel shall be distinctively uniformed while on duty and identified with their function by appropriate emblems or badges.

(2) Arms and Ammunition. All security inspectors while on duty shall be armed with a combination of handgun and ammunition which has a relative incapacitation index of at least 12.0. Such weapons shall be in serviceable condition and ready to use at all times while on duty. Additional weapons such as rifles and shotguns will be available for, and issued to, security inspector forces as necessary. There shall be at least one auxiliary weapon plus 25 percent spare weapons for each security inspector post where nuclear weapons, major weapon components, or significant quantities of SNM are involved.

(3) Storage and Maintenance of Weapons.

(a) All weapons in storage shall be securely locked in a substantially constructed container which is either fastened to the floor or wall or otherwise secured or is too heavy for easy removal. Lock and key requirements shall be as specified on page VII-1, paragraph 2d.

- (b) All weapons shall be carefully inspected by a qualified armorer at least twice a year to determine serviceability, and a record of weapons maintenance checks shall be maintained. A minimum trigger pull for firearms shall be at least that specified by the manufacturer as the minimum safety standards.

(4) Inventory of Weapons.

- (a) All issued weapons shall be inventoried by a number count on a daily basis.
 - (b) All weapons in storage shall be inventoried by a number count on a weekly basis.
 - (c) An inventory listing the type of weapon, the manufacturer, and its serial number, shall be conducted on a monthly basis. Ammunition shall be inventoried annually. The chief of the security inspector force or his or her supervisor shall attest as to the validity of the results.
 - (d) After a preliminary investigation involving an indication of unaccounted-for, missing, or stolen weapons or ammunition, the contractor shall immediately report to the cognizant field organization who shall within 24 hours report the incident to DP-34.
- (5) Firearms for Emergency Use. Firearms that are maintained on post for use during emergencies shall be under the direct control of the security inspector on duty. Such firearms shall be in a position that they will be readily accessible to the security inspector on duty but inaccessible to the persons passing through the security inspector post.

h. Use of Aerosol Irritants or Other Tear Gas.

- (1) Security inspectors and guards will be instructed in the use of aerosol irritants or other tear gas which may be provided them.
- (2) Security inspectors are authorized to use aerosol irritants or other tear gas when its use constitutes the exercise of reasonable force (that is, the minimum force, as indicated by the circumstances at the time) necessary for the discharge of their duties of safeguarding persons, classified information, classified or special nuclear material, or Government property.
- (3) In the event of use of aerosol irritants or other tear gas, care should be exercised, wherever possible, to: (a) avoid direct or close application to the eyes of any person; and (b) assure the availability of prompt medical attention to any persons affected. Any use of aerosol irritants or other tear gas must be reported within 24 hours to DP-34.

i. Access Authorization.

- (1) A Departmental "Q" Access Authorization shall be required for security inspectors assigned for the protection of nuclear explosives or significant quantities of SNM or control of access to security areas containing such materials. A "Q" access authorization shall be required for security inspectors assigned to protection of Top Secret or Secret Restricted Data, or control of access to security areas containing such matter. If there is no access to any Restricted Data in the normal course of duty, a Departmental Top Secret access authorization is acceptable in lieu of a "Q."
- (2) A Departmental "L" Access Authorization shall, as a minimum, be required for security inspectors assigned to protection of matter classified Secret National Security Information or Confidential Restricted Data, or for control of access to security areas containing such matter. If there is no access to any Restricted Data in the normal course of duty, a Departmental Secret access authorization is acceptable in lieu of an "L."
- (3) Security Clearances Granted by Other Federal Agencies may be used in lieu of a Departmental access authorization for protective personnel used in the protection of matter classified Secret or Confidential, provided there is no access to Restricted Data in the normal course of duty.

j. Orders. General and special orders shall be issued in writing covering each post, patrol, or other assignment. They shall be clear, concise, and reviewed at any time that the duties are changed, or at least semiannually to assure that they are current. Dates of such review shall be recorded on the order and initiated by the supervisor making the review.k. Supervision. Supervision of a security inspector force shall be provided to the extent required to assure proper and adequate performance of security inspector duties.

- (1) Personal Supervision. At facilities where security inspector forces of more than three security inspectors for each shift are engaged, there shall be full-time personal supervision. For shifts employing more than three security inspectors, there shall be a minimum of one supervisor for every 12 security inspectors.

- (a) Each security inspector shall be inspected by his or her supervisor upon reporting for duty to determine his or her apparent fitness for duties, including physical fitness and the condition and adequacy of his or her sidearm, uniform, or other equipment. At such time, he or she shall be given special instructions or orders as necessary.
- (b) Each security inspector post, patrol, and other activity shall be personally inspected by supervisory personnel at least twice each shift to determine that personnel and the system in general are functioning properly.
- (2) Supervision By Other Means. Various means and devices, such as recorded and supervisory tour systems, may be utilized as supplements to personal supervision or, in the case of small facilities or remote areas, to supplant personal supervision as a means of assuring that the necessary areas are patrolled and that other functions are performed.
- (3) Reports. All security inspector personnel shall report regularly to their respective Headquarters by established means of communication. Record of tours and reports to Headquarters shall be checked carefully by security inspector supervisors. Failure of a security inspector to record a visit at a designated station, to report to Headquarters as required, or other deviation from established reporting procedures, shall be investigated immediately.
- (4) Duty Log. A continuous record of all significant or unusual security inspector force activity, including details of any matters or occurrences having a bearing on the security of the facility, shall be maintained for each shift or day.

3. GUARDS.

- a. Basic Considerations. Guards may be utilized at Department and Departmental contractor administrative buildings and other locations where they do not have primary responsibility for the protection of nuclear weapons, nuclear weapon components, significant quantities of SNM, Top Secret documents, or material having similar sensitivity. When utilized, guards shall be carefully instructed in their duties and responsibilities with respect to the protection of classified matter.
- b. Duties. Guards shall observe and physically check locked repositories containing classified matter, man fixed access control points, respond to protective alarm signals, and immediately report any untoward incident involving classified matter or Government property to a supervisor.

- c. Access Authorization. Access authorization for guards shall be the same as prescribed for security inspectors set forth on page III-8, paragraph 2i.
- d. Qualification. Guards used for the protection of classified matter shall be subject to medical examination on initial assignment and at least biennially thereafter to assure their fitness to perform their duties under normal or emergency conditions. Training as specified on pages III-2, III-3, and III-4, paragraph 2d, applicable to the functions performed shall be given to guards and an appraisal reached as to the readiness to carry out the responsibilities assigned.

4. COMMUNICATIONS FOR PROTECTIVE PERSONNEL.

- a. Class A Facilities (as modified on page III-1, paragraph 2a(1)). Security inspectors at fixed posts shall have both normal telephone service and two-way radio communication with central stations as well as points from which backup forces will be dispatched. Administrative controls shall be established to assure proper use of this system in an emergency. Duress alarms shall be provided at security inspector posts.
- b. Class B Facilities. Class B facilities employing protective personnel to protect classified matter shall be provided with a system which will afford both intraplant and outside communication.
- c. Special Response Teams shall be equipped with voice privacy or digital encryption two-way radio communication.
- d. Tests. Daily tests of protective communications systems are required.

5. SECURITY INSPECTOR POST STANDARDS. Permanent security inspector posts constructed after the date of this Order for controlling access to areas containing weapons, nuclear test devices, or complete nuclear assemblies, or SNM of the types and in amounts falling within the scope of this Order shall meet the following minimum standards:

- a. Location of Security Inspector Station. Where geography and building arrangement permit, the security inspector station should be situated to provide an unobstructed view of the surrounding terrain.
- b. Exterior Wall and Door Construction. Exterior walls (excluding windows) and doors shall be constructed of or reinforced with materials which have a bullet penetration resistance equivalent to "High-Power Rifle" rating as given in Underwriter Laboratories Standard 752.
- c. Window Specifications. Windows shall consist of polycarbonate plastic and laminated safety glass or equivalent material or materials having bullet resistance equivalent to "High-Power Rifle" rating as given in Underwriter Laboratories Standard 752.

- d. Lighting Specifications. Lights shall provide a minimum of 2-foot candles luminescence at ground level for at least a 30-foot diameter circle around the security inspector post and 0.2-foot candles for 150 feet in both directions on the roadway. Sodium vapor lamps are preferred.
 - e. Vehicular Access Control. Where a security inspector station controls vehicular access to a security area, the gates and openings shall be constructed to permit closing from inside the security inspector station.
 - f. Security Inspector Posts Communication Systems. Security inspector posts should be equipped with communications systems in accordance with the requirements of paragraphs 4a and b.
6. LIMITED ARREST AUTHORITY AND USE OF FORCE BY PROTECTIVE FORCE OFFICERS. The applicable DOE policy and procedures on the exercise of arrest authority and use of force by DOE and DOE contractor protective force personnel is contained in 10 CFR 1047, "Limited Arrest Authority and Use of Force by Protective Force Officers."

CHAPTER IV
INTRUSION DETECTION

1. INTRUSION PROTECTION ALARMS.

- a. Specifications. Devices and equipment for interior intrusion detection systems required for SNM and storage of classified matter shall meet Federal specification W-H-450, "Alarm Systems, Protective, Interior," or equipment as approved by the field element.
- b. Purchase or Replacement. Purchases of new protective alarm equipment or replacement of existing equipment shall be approved in advance of purchase by the appropriate field element.
- c. Types of Alarm Systems.
 - (1) Central. A central station alarm system is one in which alarm signals are transmitted to a Headquarters location where alarm monitors are constantly attended. Such monitors shall be located at: (a) a point outside the facility such as a police station or headquarters of a commercial protective service, or (b) a plant protective force station serving the facility.
 - (2) Local. A local alarm system is one which employs a loud, audible signaling device, such as a siren or bell, in the immediate vicinity of the protected area. It may be used only when buildings, vaults, rooms, or containers requiring alarm protection are so located that the signal would be immediately detected by personnel designated to take necessary protective action. Tests shall be conducted at least monthly, and appropriate records shall be maintained. These tests shall also include personnel detection of the audio signal and appropriate response.
- d. Central Station Operating Requirements.
 - (1) Response to Alarms. Response to alarms shall be timely with site-specific tests made to assure compatibility with the intent of timeliness. Results of the response times from the site-specific tests shall be incorporated in the security survey report of the facility.
 - (2) Tests.
 - (a) Alarm equipment and circuits shall be tested at least once a week by actual intrusion of the alarmed area or

object. Alarms caused by the opening and closing of areas by operating personnel in the normal performance of their activities are acceptable tests.

- (b) When a number of electromechanical devices are used, such as tamper door, and window switches in a single (series) circuit, testing of these switches on a rotational basis is recommended to assure complete test of the circuit within a reasonable period of time.
 - (c) When volumetric or proximity sensors are used, sensitivity and walk tests shall be conducted as determined by the Heads of Field Elements to assure that the degree of required sensitivity is maintained and that the area requiring protection is adequately covered.
 - (d) Tests shall be conducted at least semiannually to determine the response time by the protective force and, if applicable, as frequently as feasible to determine the response time by commercial protective service personnel.
 - (e) Records shall be maintained of the tests of alarm equipment and circuits. The records shall include the date of the test, name of person conducting the test, and the results.
 - (f) False and nuisance alarm rate records shall be maintained and results analyzed to determine alarm system performance.
- (3) Inspection. Alarm equipment and circuits shall be thoroughly inspected by qualified service personnel at least annually to assure continuing operability and reliability.
- (4) Service. All alarm equipment and circuits shall be serviced and maintained by qualified service personnel who possess appropriate access authorizations as cited in subparagraph (5)(c) below.
- (5) Access Authorization.
- (a) Plant protective force personnel responding to intrusion detection alarms used for the protection of classified matter located within exclusion areas shall possess "Q" access authorizations when Top Secret or Secret matter or SNM is involved and "L" access authorizations, as a minimum, when Confidential matter is involved. If access is not to SNM or Restricted Data, security clearances at the appropriate level granted by another Federal agency and certified to the Department may be accepted in lieu of a "Q" or "L" access authorization.

- (b) Plant protective force personnel monitoring any alarm equipment or responding to intrusion detection alarms used for the protection of classified matter in limited or nonsecurity areas shall possess, as a minimum, "L" access authorizations. Security clearances granted by another Federal agency and certified to the Department may be used in lieu of the "L" access authorization. To the extent feasible, assurance of the dependability and reliability of police or commercial protective service personnel monitoring or responding to alarms shall be obtained.
- (c) Maintenance personnel performing any type of work on intrusion detection alarms or alarm equipment used for the protection of classified matter shall possess an access authorization equivalent to those cited in subparagraphs (a) and (b), above, for plant protective force personnel, for the areas, levels of classified matter, and/or SNM to which they will have access.
- (6) Recordkeeping. Protective force personnel shall record each nonscheduled alarm, showing the date and time the signal was received, the time protective or other responsible personnel arrived at the alarmed area, action taken, and the cause of the alarm if known, or probable cause if not definitely established. The name and signature of the recorder and date of recording shall appear in such record.
- e. A Report of Each Nonscheduled Alarm shall be furnished to the facility security officer immediately if unauthorized intrusion is involved and a report made immediately to the cognizant field element. Otherwise, the report shall be furnished to the facility security office on the same day if such alarm occurs during normal working hours or no later than the first working day after such alarm when it occurs during nonworking hours.
- f. Power Sources.
 - (1) A primary and auxiliary power source is required for protective alarm systems.
 - (2) Auxiliary power for protective alarm systems shall be supplied by batteries or engine driven generators. Switchover to the auxiliary power shall be automatic upon failure of the primary power source, and upon failure of both the primary and auxiliary power sources a signal shall be generated to indicate an alarm condition at the monitor.

- (3) Rechargeable batteries shall be kept fully charged or subject to automatic recharging whenever the voltage drops to a level specified by the battery manufacturer. Nonrechargeable batteries shall be replaced whenever the voltage drops 20 percent below the rated voltage. A signal shall be activated in the monitor to indicate when this condition exists.
 - (4) Auxiliary power sources shall be capable of maintaining full operation of the alarm system for not less than 8 hours. Such power sources shall contain a switching capability to facilitate operational testing as determined by the Head of Field Elements to determine adequate emergency power sources and shall be maintained by qualified service personnel.
 - (5) The power supply, other than public utility, shall be vented sufficiently to preclude deterioration of any of its components as a result of operation under high temperatures.
- g. Alarm Line Supervision. Line supervision limits and/or line tamper alarm capability shall be specified as follows:
- (1) For the protection of classified matter: Underwriter Laboratories' Class AA requirements shall be met.
 - (a) A Departmental facility, contractor, or subcontractor possessing classified information under the protection of a central station alarm system shall have its alarm connected by direct, continuously supervised leased line or by such other means so as to distinguish its alarms from all other customers of that central station.
 - (b) The line shall be continuously supervised so as to detect any attempts to short, open, or substitute a bogus signal for the legitimate "no alarm" signal in a surreptitious attempt to bypass the alarm system.
 - (2) For the protection of Category I or II amounts of SNM:
 - (a) For existing systems:
 - 1 Direct or alternating current with continuous line supervision adequate to detect a short, open, or substitution shall be the minimum used, provided that all equipment containers, junction boxes, and so forth, are tamper resistant and alarm wiring is contained in rigid wall metal conduit. Digital line supervision is, however, preferred over direct or alternating current supervision.

- 2 The system shall be capable of detecting tamper with the system, any component, or the line in both the secure and access modes.
- 3 Interface components such as line modems, or data gathering panels shall be located, if practical, either at the central annunciating point or in the protected area. All field located components e.g., line amplifiers shall be tamper protected and preferably buried or located within a building.
- 4 If dedicated telephone cable pairs are used to connect the protected area to the annunciating point, they must not be routed through telephone switching equipment. Where connected through frame rooms, the pairs shall not be identified as alarm system pairs.

(b) For new systems:

- 1 A continuously polled, digital interrogation/response, transmission system shall be used.
- 2 Each protected zone shall have a unique digital address code.
- 3 The polling shall be in a pseudorandom manner (i.e., all zones are polled during each sequence but the order or start point is varied). Alternately, encryption may be used.
- 4 The interface equipment shall be protected as specified in sub paragraph 1g(2)(a)3, above. Also, the interface equipment shall be capable of initiating an alarm if any malfunction or tamper occurs while in both the access or secure modes.
- 5 The polling sequence shall poll all protected zones at the fastest rate consistent with the type of transmission media used (e.g., coaxial cable, radio, or telephone pairs).
- 6 A redundant and separately located transmission line shall be installed. If two cables are utilized, they shall not be installed in the same trench.

2. PROTECTIVE LIGHTING.

- a. Protective lighting, as a part of a security system, should be used as pertinent for proper physical protection of classified matter.

- b. Lamps in which light is produced directly or indirectly by the use of gas, such as sodium vapor lamps, are highly efficient and economical in operation, and their use in protective lighting systems is encouraged. However, it should be recognized that gas lights require a relight period of approximately 3 minutes following any power interruption.
- c. Facilities requiring protective lighting shall have an emergency lighting capability of the type and size required in relation to the importance of the facility, reliability of regular power sources, and feasibility of using portable lighting equipment.
- d. Where protective lighting at remote perimeters is not feasible, protective force patrols and fixed stations may be equipped with night vision devices, although it should be recognized that adequate perimeter lighting provides better protection and deterrence to intrusion than do such devices. Night vision devices shall not be used in lieu of protective lighting at ingress and egress points.
- e. Adequate illumination shall be provided to detect intruders, reveal unauthorized persons, and, at pedestrian and vehicular entrances, to permit examination of credentials and vehicles.
- f. Light glare shall be kept to a minimum in those situations where it would impede effective operations of protective force personnel, interfere with rail, highway, or navigable water traffic, or be objectionable to occupants of adjacent properties.
- g. Light sources on perimeters shall be so located that illumination is directed, whenever possible, outward and with relative darkness existing along patrol routes and at fixed posts other than pedestrian and vehicular entrances.

CHAPTER V

PHYSICAL PROTECTION OF CLASSIFIED MATTER

1. PHYSICAL PROTECTION OF CLASSIFIED MATTER IN USE.

- a. Classified matter shall be located within limited or exclusion areas unless those using the matter can protect it against unauthorized access outside of such areas.
- b. Classified matter shall not be removed from a limited or exclusion area without authorization as set forth in DOE 5635.1.
- c. Classified matter in use shall be constantly attended by, or under the control of, appropriately cleared personnel concerned with its use.
- d. Persons attending or controlling classified matter shall prevent unauthorized persons from having access to the matter.
- e. Classified matter in use shall be protected against unauthorized visual access when classified information can be obtained by observation of the matter.
- f. Where required, an accountability system shall be maintained to reveal promptly when classified matter is lost or unaccounted for. Action shall be taken to recover or ascertain the actual disposition of unaccounted for matter or otherwise resolve discrepancies between records and actual quantities on hand.
- g. Classified material and equipment shall bear classification and extra markings either by stamping, tags, labels, or other suitable means.
- h. Classified automatic data processing systems information requires additional safeguarding as set forth in DOE 5636.2 and DOE 5636.4.
- i. Any inability to account for or any loss of classified matter shall be reported in accordance with DOE 5633.1.
- j. Provisions for limited or exclusion area exit searches of handcarried items shall be made.

2. PROTECTION OF CLASSIFIED MATTER IN STORAGE.

- a. Basic Considerations. Although classification is the only security factor determining the degree of protection required for classified matter in storage, the following factors, in addition to classification, shall be considered:

- (1) Strategic importance;
- (2) Susceptibility to compromise;
- (3) Effect on vital production or delivery schedules;
- (4) Health and safety factors; and
- (5) Replacement cost.

b. Security Containers.

- (1) Specifications. Security containers required for the storage of classified matter shall, as a minimum, conform to the following specifications:
 - (a) A security cabinet is one which bears a test certification label on the inside of the locking drawer or door and is marked "General Services Administration Approved Security Container" on the outside of the top drawer or door.
 - (b) A safe is a burglar-resistant cabinet or chest having a body of steel at least 1/2-inch thick and a built-in, three position, changeable combination locked steel door at least 1-inch thick exclusive of bolt work and locking devices.
 - (c) A vault is a burglar-resistant, windowless enclosure that meets the definition of an SNM vault as given in this Order. Additionally, vaults should include an intrusion alarm system activated by an opening of the door.
 - (d) A vault-type room is one having a combination locked door and protected by an intrusion alarm system activated by any penetration of walls, floors, ceilings or openings, or by motion within the room.
 - (e) Built-in combination locks on security containers specified in subparagraphs 2b(1)(a), (b), and (c) shall meet Underwriter Laboratories' Standard No. 768, Group 1-R.
- (2) Transfer of Security Containers. When a security container is transferred from one organization to another, for any purpose, 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 organizational level at which this requirement shall apply (e.g., branch, division, office) is to be determined by each organization's security office.

c. Requirements for Storage.

- (1) Top Secret Matter, while unattended or not in actual use, shall be under continuous armed protective force control or stored in security containers:
 - (a) Located within a guarded limited or exclusion area under either central station alarm protection as prescribed in this Order or armed protective force patrol and inspection of each container at intervals not to exceed 4 hours.
 - (b) Not located within a limited or exclusion area but under central station alarm protection as prescribed in this Order and armed protective force patrol at intervals not to exceed 2 hours.
- (2) Complete Nuclear Weapons, complete nuclear weapon configurations without nuclear material and nuclear test devices, while unattended or not in actual use, shall be under continuous armed protective force control or stored in security containers located within a guarded material access area under alarm system protection.
- (3) Secret Matter, while unattended or not in actual use, shall be stored in a manner authorized for Top Secret matter or at least as secure as one of the following:
 - (a) With respect to documents not located within a security area, in a security container under alarm protection as prescribed in this Order or protective force patrols as set forth in subparagraph (8) below.
 - (b) With respect to documents located within a limited or exclusion area or other area under protective force control during nonworking periods:
 - 1 In a security container or a commercial-type steel filing cabinet equipped with a built-in, changeable combination lock under alarm protection as prescribed in this Order or protective force patrols at intervals at least once during

each 24 hours of a nonworking period exceeding 1 day. In the case of Class A facilities which have the repositories in security or guarded areas, the protective force shall physically inspect at least 25 percent of the repositories daily on a rotational basis.

- 2 In unlocked cabinets or open storage within a vault or vault-type room.

(c) With respect to materials, components, and equipment where size, weight, or construction offers substantial resistance to unauthorized removal or surreptitious access to contents:

- 1 In a locked building of substantial construction or in a locked room within such building when the room or building is under alarm protection or subject to random guard patrols as prescribed in this Order.
- 2 In open storage within a securely locked and separately fenced security area which is located within a larger limited or exclusion area, when the classified information is concealed from unauthorized persons and the storage area is subject to protective force patrol and inspection at intervals not to exceed 4 hours.
- 3 In open storage within a limited or exclusion area which is not located within a larger limited or exclusion area, but is enclosed by a physical barrier as prescribed in this Order, when the classified matter is concealed from unauthorized persons and the storage area is subject to protective force patrol and inspection at intervals not to exceed 2 hours.

(d) With respect to materials, components, and equipment which are susceptible to unauthorized removal or surreptitious access in a manner set forth in subparagraphs 2c(3)(a), (b), and (c) except that protective force patrol, when required, shall occur at intervals not to exceed 2 hours.

(4) Confidential Matter, while unattended or not in actual use, shall be stored in a manner authorized for Secret matter or at least as secure as one of the following:

(a) With respect to documents:

- 1 In a security container or commercial-type steel filing cabinet equipped with a built-in, changeable combination lock or lock bar and combination padlock.

- 2 On shelves or tables within a locked room, or in a key-locked filing cabinet, when the room or cabinet is under alarm protection or protective force patrol, as prescribed in this Order.
 - (b) With respect to materials, components, and equipment:
 - 1 In a securely locked building of substantial construction.
 - 2 In open storage within a limited or exclusion area, provided the classified matter is concealed from view and the storage area is subject to protective force patrol and inspection at intervals not to exceed 4 hours.
 - 3 In a security container or commercial-type steel filing cabinet equipped with a built-in combination lock or lock bar and combination padlock.

(5) Communications Security Matter, while unattended or not in actual use, shall be stored in a manner authorized above for the classification involved and, in addition, shall meet the requirements set forth in DOE 5300.3A.

(6) Sensitive Compartmented Information Facilities shall be afforded physical protection in accordance with the DOE Procedural Guide, "Security Standards for Sensitive Compartmented Information and Facilities." Any matters pertaining to this subject shall be referred to DP-34 for coordination.

(7) When protective forces are required for the protection of Departmental interests at facilities having unalarmed repositories containing Secret or Confidential matter, they shall physically inspect such repositories as soon as possible after the close of each normal workday and at least once every 24 hours of a nonwork period exceeding 1 day. In the case of Class A facilities which have the repositories in security or guarded areas, the protective force shall physically inspect at least 25 percent of the repositories daily on a rotational basis.

(8) Areas containing Secret matter in open storage or other matter requiring patrols shall be subject during nonwork hours to protective force patrols at such intervals as deemed necessary, taking into full consideration the sensitivity and quantity of the matter involved, but in no event less frequently than once during each 8-hour shift.

d. Alternate Storage Locations.

- (1) Safe Deposit Box/Vault of a bank 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. Such persons must be appropriately cleared for the level of classification involved.
- (2) Remote Storage Facilities, such as an "offsite" emergency relocation center or underground facility in a remote location, shall be provided with safes, vaults, or security containers for the storage of classified matter.
- (3) Federal Records Centers may be used for the storage of classified information. Refer to DOE 5635.1.

e. Locking and Monitoring of Repositories and Office Areas.

- (1) All classified matter must be properly secured when the office is unattended.
- (2) The names, addresses, and telephone numbers of custodians having knowledge of the combination shall be posted on the inside or outside of each combination-locked repository containing classified matter. A record of the date of last change of the combination shall be posted on the outside of each repository.
- (3) A monitor sheet containing spaces for initialing by the locker and the monitor shall be posted on each cabinet or repository containing classified matter or, if one monitor sheet includes several such repositories located in the same area, it may be posted in a conspicuous place in the area. The monitor sheet shall be initialed at the end of each workday by the person responsible for locking the repository(ies) and, except when not feasible, by one other person who has physically checked the lock(s), locked door(s), or drawers to assure proper securing of the repository(ies).
- (4) In the event that an unattended repository containing classified matter is found open, one of the custodians shall be notified immediately, the repository shall be secured by a designated protective force person, and the contents shall be checked not 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 evidence, and an immediate report shall be made as required by DOE 5633.1.

- f. Retention of Classified Matter After Termination of Contract.
Classified matter retained after termination of a contract, subcontract, or other agreement shall be safeguarded in accordance with the provisions of this Order. A certificate of possession shall be executed. Refer to DOE 5634.1.

3. PROTECTION OF CLASSIFIED MATTER IN TRANSIT.

a. Basic Considerations.

- (1) The principal hazards to security shipments are espionage, sabotage, terrorism, collision, theft, damage, improper routing, and misdelivery.
- (2) Security shipments containing classified matter require protective surveillance by the Department, Departmental contractor, or commercial carrier personnel to prevent delays or losses in transit.
- (3) Approved classified shipping addresses are necessary to assure proper handling upon delivery of a security shipment to the consignee.
- (4) Classified documents shipped in bulk are considered to be security shipments subject to the provisions of this part.
- (5) Security shipments containing communications security information require security measures as set forth in DOE 5300.3A.

b. Protective Services Available for Departmental Security Shipments.

- (1) In Custody of the Department or Departmental Contractor Personnel.
 - (a) Departmental or Departmental contractor personnel, designated by name or title and upon written authority may handcarry Secret or Confidential matter between facilities under procedures approved by the responsible Heads of Departmental Elements. Personnel carrying this material shall conduct themselves in such a manner that the security of the matter entrusted to them will not be prejudiced through carelessness, inadvertence, or lack of vigilance and shall keep the classified documents continuously in their custody.
 - (b) The Department or Departmental contractor personnel may transport or escort Secret or Confidential shipments between limited or exclusion areas or between a security facility and a nearby transportation terminal.

- (c) Department or Departmental contractor personnel may transport or escort Secret or Confidential matter between security facilities provided that the matter is appropriately and securely packaged, that classified information is not open to view, and that the shipment moves in a sealed van-type vehicle or other type equivalent service and is under the control of personnel responsible for its custody at all times while in transit.
 - (d) Personnel specified in subparagraphs 3b(1)(a), (b), and (c) shall possess "Q" access authorization for transporting Secret matter or at least an "L" access authorization for transporting Confidential matter. If there is no access to "Restricted Data," an "L" access authorization is sufficient for transporting the Secret matter. A DOD final Secret clearance may be used in lieu of a "Q" or "L" access authorization, respectively, provided there is no access to Restricted Data.
- (2) The various classes of mail, special protective services available, and instructions for using them are set forth in the Federal Property Management Regulation, 41 CFR 101-11.3.
 - (3) Railroad, truck, or airlines may be used for the shipment of material upon the approval of the service by the responsible Heads of Departmental Elements, based upon protection meeting the minimum security requirements outlined in subparagraphs (a) through (e) below.
 - (a) Spot checks shall be conducted periodically to verify compliance with the minimum security requirements.
 - (b) Classified matter shall be packaged and so banded, sealed, or otherwise fastened so that any attempted opening or unauthorized inspection would be readily revealed.
 - (c) Any losses of classified matter, possible violations or any other unlawful activity resulting from the use of such service must be reported immediately to DP-34.
 - (d) Other modes of transportation and postal service may be used upon the approval of the Heads of Field Elements, with the concurrence of DP-34.
 - (e) As a minimum, the common carrier shall provide all of the following security services:
 - 1 Surveillance by an authorized carrier employee when the classified matter is outside the vehicle.

- 2 A hand-to-hand signature receipt system which assures the prompt tracing of the shipment while en route.
- 3 When storage is required, classified matter must be stored in an alarmed or guarded storage area with immediate response by a carrier employee, commercial guard, or police.
- 4 Verification of the identity and authorization of persons who pick up the classified matter.
- 5 Pick up and delivery by a vehicle which provides basic concealment. When a van is used, the van shall be locked while in transit.

c. Security Shipment Conditions. Approved means of shipment for classified matter set forth below are subject to the following conditions:

- (1) Contents shall be securely packaged, including double wrapping, where practicable, and shall meet appropriate regulations regarding structural strength and materials.
- (2) Contents shall be so packaged that attempted opening or unauthorized inspection shall be readily detected en route or upon arrival at destination.
- (3) Contents shall be checked against shipping papers as promptly as practicable after arrival. Any unresolved discrepancy shall be reported immediately to the responsible Heads of Field Elements, or in the case of Headquarters, to DP-34.
- (4) The classification of the contents shall be indicated, unless prohibited by health considerations, inside the package or container to preclude errors in handling and storage after delivery.
- (5) Tamper-resistant seals shall be used whenever practicable and shall be placed on car or van doors, containers, or other positive fastening devices by, or in the presence of, a Department or Departmental contractor representative. Seals shall be serially numbered and distinctively designed, and appropriate entry shall be made in bills of lading or other shipping papers. Seal numbers shall be verified by the consignee upon arrival.
- (6) Combination padlocks shall be used whenever practicable on closed vehicles in addition to seals.
- (7) Receipts, listings, and other papers revealing classified information shall be appropriately marked.

- (8) Shipping or transfer documents which could reveal classified weights or quantities of material shall be appropriately classified.
- (9) Matter in the custody of escorts shall be under their control until delivered or placed in storage.
- (10) Notification of shipments of Top Secret matter, together with sufficient information to enable proper handling at the destination, shall be transmitted to the Departmental Element at the destination exercising administrative jurisdiction over the consignee, prior to departure of the shipment.
- (11) Notification of Secret or Confidential shipments, other than packages sent by mail, shall be transmitted prior to departure either to the consignee or to the Departmental Element exercising administrative jurisdiction over the consignee, with sufficient information to enable proper handling at destination.
- (12) Secret or Confidential shipments received at common carrier terminals shall be picked up by the consignee during the same working day or next working day if received after working hours, unless the carrier provides continuous protective service to the address of the consignee.
- (13) Unescorted carload shipments via rail shall be made under arrangements with carriers to furnish passing reports identifying the location of cars at designated times and points and to provide prompt notification of any delay or incident which may interfere with the scheduled arrival of cars at their destinations. Exceptions may be made to these requirements when the arrangements would be unproductive for the Department and unreasonably burdensome to the carrier.
- (14) Unescorted truckload shipments shall be made under arrangements with carriers to provide in-transit reports when they would serve a useful purpose and immediate notice concerning any breakdown or other serious delay.

d. Approved Means of Shipment.

(1) Security Shipments Moving Entirely Within the United States.

- (a) Nuclear weapons, Category I and classified Category II SNM, and Top Secret matter, excluding Top Secret communications security matters, shall be transported in the custody of Department-approved armed couriers. "L," "TS," or "S" access authorizations may be substituted if Secret National Security Information only is involved.

- (b) Top Secret communications security matter may be transported in the custody of two escorts, either Department or Departmental contractor personnel. These escorts need not be armed nor must they meet security standards applicable to Departmental couriers. However, they must, as a minimum, possess the appropriate access authorization, i.e., "TS" access authorization for escort of TS/NSI matter and "Q" access authorization for escort of TS/RD matter.
- (c) Secret matter shall be transported by one of the following:
 - 1 Departmental courier;
 - 2 U.S. registered mail;
 - 3 In custody of Department or Departmental contractor personnel having "Q" access authorization;
 - 4 Aircraft under Departmental contract with pilots holding "Q" access authorization, or U.S. Government aircraft with pilots who hold "Q" access authorization or DOD or other U.S. Government agency final Secret clearance and who maintain continuous custody of the matter entrusted to them;
 - 5 Commercial carriers including:
 - a Motor carriers in exclusive use that provide locked and sealed van service with two "Q" cleared drivers, assurance that the drivers will maintain contact with the carrier dispatcher at a minimum of 4-hour intervals or as otherwise specified by the Department or the Departmental contractor office, and the shipment will be constantly attended by at least one "Q" cleared driver. In some instances, the field element may approve the use of "L" or other U.S. Government agency cleared drivers if the drivers will have no access to the classified contents under normal circumstances.
 - b Locked and sealed railroad cars; carrier shall furnish, on request, a passing report identifying the car's last location; or
 - c Air carriers under conditions allowing for prompt tracking and special signature services.

- 6 Other modes of transportation and postal or express service may be used upon the approval of Heads of Field Elements with concurrence of DP-34.

(d) Confidential matter shall be transported by one of the following:

- 1 In a manner authorized for matter of higher classification;
- 2 U.S. first-class express or certified mail;
- 3 Airlines under Departmental contract, or U.S. Government aircraft, with pilots holding "L" access authorization or DOD or other U.S. Government agency final Secret clearance;
- 4 Common carrier service (rail, truck, or air), as approved by the Heads of Departmental Elements and the minimum requirements as specified in this Order;
- 5 Other modes of transportation and postal or express service, upon approval of the Heads of Field Elements and with the concurrence of DP-34; or
- 6 Rail, truck, or air without escort, access authorization, or special protective services when loaded containers weigh more than 500 pounds, or when size and weight together preclude removal without the aid of mechanical devices, and the containers are securely banded, sealed, and otherwise fastened so as to reveal readily any attempted opening or unauthorized access.

(2) Security Shipments Outside the United States.

- (a) Top Secret matter, complete nuclear weapons, complete weapons configurations without nuclear material, and nuclear test devices shall be transported in the custody of Departmental couriers, provided that the aircraft or vessel used shall be under U.S. registry or U.S. military control.
- (b) Secret or Confidential matter shall be transported:
 - 1 In a manner authorized for Top Secret matter;
 - 2 Via U.S. registered mail through U.S. military or civil postal facilities, provided the material does not pass through a foreign postal system; or

- 3 By any mode of transportation approved by the Department for shipments within the United States, provided the shipments are under U.S. Government custody and control.
- (c) Security shipments to weapon test sites shall be transported between Departmental or military installations within, and weapon test sites outside, the U.S. in a manner at least equivalent to that set forth in subparagraphs (2)(a) and (b), above, and approved by the Manager, Nevada Operations Office, or the commander of the task force concerned.
- (d) Security shipments between the United States and foreign countries:
- 1 Classified matter, except as provided in subparagraph 2, below, shall be transmitted to foreign countries only after DP-34 has approved the means of transportation.
- 2 Secret or Confidential matter transmissible by mail shall be sent between U.S. Government installations in the U.S. and Canada, and Canadian installations in Canada, by U.S. or Canadian registered mail.
- e. Receipts. The following receipts, as appropriate, shall be used for the transfer of classified matter outside security areas:
- (1) The standard Departmental courier receipt; or
- (2) An appropriate receipt for the classified matter, showing date of transmittal and an adequate unclassified identification of shipper, receiver, and material transmitted.
- f. Courier and Escort Duties (These do not include the courier duties of the Federal couriers in the Transportation Safeguards Division.)
- (1) Courier duties may be performed by a Departmental employee or member of the Armed Forces who is assigned to and performing duties under the discretion and control of the Department. Persons performing courier duties shall possess a "Q" access authorization or an equivalent DOD security clearance, shall be authorized under section 161k of the Atomic Energy Act of 1954, as amended, or other appropriate statutory authority to carry firearms and make arrests without warrant, and shall be specifically charged with the armed protection of designated matter in transit.
- (2) Escort duties may be performed by a Department or Departmental contractor or common carrier employee specifically assigned for the delivery of a security shipment. Escorts may include guards, truck drivers, and other attendants furnished by the Department, Departmental contractors, or common carriers.

- (3) Couriers shall be "Q" cleared. Other escorts, used as assistants to couriers for the protection of Top Secret shipments, or responsible for the protection of Secret shipments shall possess a "Q" access authorization or, if there is not access to Restricted Data, "L" or "S" access authorization. Escorts responsible for the protection of Confidential shipments shall possess, as a minimum, a "L" access authorization or, if there is no access to Restricted Data, an appropriate clearance of another Federal agency.
- (4) Individuals assigned escort duties for the protection of security shipments shall:
 - (a) Carry packages on the person, or in handcarried containers, until delivered to consignee or placed in approved storage.
 - (b) When accompanying classified matter in a freight car, provide continuous observation of the containers and observe adjacent areas during stops or layovers.
 - (c) When traveling in an escort car accompanying a security shipment via rail, keep the shipment cars under observation and detrain at stops, when practicable and time permits, to guard the shipment cars and check car or container locks and seals.
 - (d) Maintain liaison, as required, with train crews, other railroad personnel, special police, and law enforcement agencies.
 - (e) When escorting security shipments via motor vehicle, maintain continuous vigilance for the presence of conditions or situations which might threaten the security of the cargo, take such action as circumstances might require to avoid interference with continuous safe passage of the vehicle, provide assistance to, or summon aid for, crew of cargo vehicles in case of emergency, check seals and locks at each stop where time permits, and observe vehicles and adjacent areas during stops or layovers.
 - (f) When escorting shipments via commercial or military aircraft, provide continuous observation of plane and cargo during ground stops and of cargo during loading and unloading operations.
- (5) A sufficient number of couriers or other escorts required to perform the above functions shall be assigned to a shipment, including sufficient relief personnel.

- (6) To obtain maximum economy and efficiency in the use of shipment personnel, escorted security shipments of two or more offices moving in the same direction within the same time period, should be merged, when feasible, into one shipment operation under the protection of one escort crew.

(7) Firearms.

(a) Requirements for Arming.

- 1 Individuals performing courier duties shall be armed, as a minimum, with a handgun and ammunition which has a relative incapacitation index of at least 12.0 at all times while having custody of Top Secret matter and, in addition, with auxiliary weapons (rifle and shotgun) at all times while having custody of nuclear weapons, nuclear test devices, or complete nuclear weapon configurations without nuclear materials.
- 2 Individuals performing escort duties, other than couriers, will be appropriately armed at all times when assisting couriers in the protection of Top Secret matter, complete nuclear weapons, weapon configurations without nuclear materials, or nuclear test devices.

(b) Handling of Firearms.

- 1 Firearms shall be carried or transported as inconspicuously as possible.
- 2 Any incident arising from the possession or use of firearms by individuals performing courier or other escort duties on official duty will be reported immediately to the responsible Head of the Field Element, who shall, in turn, report the incident and any action taken or contemplated to DP-34.

- (c) A firearm shall not be issued to a Departmental employee until the responsible Head of the Departmental Element has assured himself or herself that the individual who is to receive it is fully competent and reliable, and has qualified in the use of firearms in accordance with Departmental firearms standards.

(d) Firearms Qualification.

- 1 Every person designated as a courier or escort by the Department shall fire a familiarization course of at least 100 rounds at least semiannually and shall qualify at least annually with their issue handguns and ammunition.

The combination of handgun and ammunition shall have a relative incapacitation index of at least 12.0. This requirement does not apply to Transportation Safeguards Division Couriers who have their own standard.

- 2 Administrative couriers (i.e., those who, under emergency conditions or when time is a controlling factor, must carry Top Secret documents) shall qualify at least annually with a handgun and ammunition which shall have a relative incapacitation index of at least 12.0. The number of persons serving as administrative couriers shall be maintained at an absolute minimum consistent with operational requirements.
- (e) If a courier or escort is to be armed with auxiliary weapons during the course of his assigned duties, he or she shall fire a familiarization course of at least 50 rounds with each type of auxiliary weapon at least semiannually.
- (f) Couriers and escorts shall not be issued firearms until they have demonstrated their proficiency under the requirements set forth in subparagraph (7)(d), above and have received appropriate safety training in the use of the weapons to be carried. Couriers who have been issued firearms previously but who fail during annual qualification tests to meet the minimum standard may be given additional instruction and further opportunities to qualify within a 6-month period.
- (g) A firearms qualification record shall be maintained for each courier or escort who qualifies under subparagraph (7)(d), above. Each record shall be retained until the next qualifying scores are entered on a new record and placed in the courier's file. Current records shall be retained for at least 1 year after separation of a Departmental employee from courier duties.
- (8) Section 161k of the Atomic Energy Act of 1954, as amended, authorizes the appropriate arming of Department and Departmental contractor personnel, as necessary, for the protection of matter in their custody.
- (9) Courier and Escort Identification.

 - (a) Couriers and escorts shall possess identification cards issued by the Heads of the Field Element (or DP-34 for Headquarters). They shall carry them at all times while in custody of security shipments. These cards shall be safeguarded, and the loss of a card shall be reported immediately to all Heads of Departmental Elements.

- (b) Any courier authorized to carry a firearm aboard a commercial or public-owned aircraft shall comply with the rules and regulations set forth in 14 CFR 108.
- (10) Escorts shall conduct themselves throughout each security shipment operation in such manner that the security of matter entrusted to them shall not be prejudiced through carelessness, inadvertence, or lack of vigilance. Use of intoxicants by escorts while assigned to a security shipment operation is prohibited.
- (11) Specific instructions and operating procedures shall be prepared in detail and issued to escorts prior to each shipment. The following items are suggested for inclusion:
 - (a) General outline of the mission;
 - (b) Name and address of persons, including alternates, to whom the classified matter is to be delivered;
 - (c) Receipt to be obtained from consignee;
 - (d) Means of transportation to be used;
 - (e) Number of couriers and other escorts, if any;
 - (f) Duties of each courier or other escort during movement, during stops en route, and during loading and unloading operations;
 - (g) Communications procedures;
 - (h) Emergency procedures, including the use of firearms and instructions for obtaining relief in the event of incapacitation or other personal emergency; and
 - (i) Health and safety precautions.

CHAPTER VI

PHYSICAL PROTECTION OF SPECIAL NUCLEAR MATERIAL

1. BASIC CONSIDERATIONS.

- a. This chapter applies to all special nuclear material which is in the possession of Departmental Elements or Departmental contractors, subcontractors, or consultants, and which is not subject to license by the Nuclear Regulatory Commission (NRC).
- b. Physical protection afforded to Departmental SNM in the civilian reactor program shall be comparable in effectiveness to that required by NRC for its SNM licensees.
- c. The standards, procedures, and requirements of this chapter are minimum requirements. In establishing physical protection systems within each category of SNM, application of this chapter should consider the relative attractiveness of characteristics such as ease of accessibility and concealment, portability, chemical purity, isotopic purity, radioactivity, and chemical and physical form.
- d. Specific hostile actions to be protected against involving SNM include:
 - (1) Theft of SNM, i.e., unauthorized removal from a material access area, protected area, or from an SNM shipment.
 - (2) Diversion of SNM, i.e., unauthorized placement of SNM within a material access area or protected area.
 - (3) Sabotage of an SNM facility or shipment which would result in unacceptable impact on programs or unacceptable impact on the public health and safety.
- e. Based on paragraph 1d above, consideration must be given to exclusion containment, and neutralization strategies for the range of hostile activities.
- f. Controls shall be established to protect against unauthorized access to or removal of SNM.
- g. Access to SNM shall be limited to persons who possess appropriate access authorization, certification, or verification, and who require such access in the performance of their official duties.
- h. The number of persons provided such access shall be kept to an absolute minimum consistent with efficient execution of authorized operations, and with the surveillance requirements of this Order.

2. SPECIAL CONDITIONS. DOE 5630.2 provides a Category IA and IB; this Order provides a Category IIIA & IIIB. Reconciliation of these facts, particularly as it relates to accumulation of SNM (rollup) will be provided in future guidance from the Office of Safeguards and Security. Under certain conditions, the levels of physical protection required by this Order may be reduced. When planning and implementing a physical protection system with respect to special conditions, consideration must be given to prevention of theft, diversion, and sabotage.
- a. When considering prevention of theft or diversion, the following special conditions may allow for a reduction in levels of physical protection:
- (1) The SNM is not readily separable from other radioactive material, and the combination of the SNM and other radioactive material delivers an external radiation dose of approximately 100 rems per hour or more at 1 meter from any accessible surface without intervening shielding material.
 - (2) The SNM is contained in material that has been declared as waste.
 - (3) The SNM is in a chemical, isotopic, or physical form or is within isolated in-process, or remote, inaccessible containment which provides physical protection that is comparable to the protection required by this Order.
- b. When considering prevention of sabotage, however, if the severity of the risk and consequences are deemed unacceptable, the above conditions may not provide adequate protection for the prevention of unauthorized access to and seizure of SNM or an SNM facility for purposes of sabotage. Special conditions for reducing protection levels with respect to preventing sabotage include the following:
- (1) Geographic isolation which would mitigate adverse programmatic, or health and safety impacts of an act of sabotage.
 - (2) Natural or manmade containment which provides adequate physical barriers to unauthorized access or prevents the dispersal of SNM.
 - (3) Other special considerations which would serve to mitigate the potential for, or consequences of, sabotage (to be evaluated on a case-by-case basis).
- c. Where the foregoing conditions exist, they should be specifically and clearly described in the site-specific safeguards and security plan to demonstrate a logical basis for the physical protection system provided. When material is to be shipped, it shall be the responsibility of the shipper to determine if any of these conditions exist. At certain facilities, a level of physical protection exceeding that specified herein may be necessary in order to assure a satisfactory level of protection.

3. GENERAL REQUIREMENTS.

- a. A facility shall not receive, use, process, or store SNM until an SNM facility approval, based upon a review and acceptance of the safeguards and security plan and an onsite survey by the responsible operations office, has been granted.
- b. Continual vigilance shall be maintained for procedural violations or practices inconsistent with physical protection measures afforded SNM.
- c. Any unauthorized attempts, suspected attempts, or actual removals of special nuclear material from a security interest shall be reported immediately to the responsible safeguards and security office.
- d. Reports, plans, and data relating to the protection and control of SNM shall be classified in accordance with Classification Guides CG-SS-1 and CG-TSS-1.

4. PROTECTION OF CATEGORY I QUANTITIES OF SPECIAL NUCLEAR MATERIAL - IN USE OR STORAGE. (Categories of SNM are summarized in Attachment VI-1.)

- a. Category I quantities of SNM shall be used, processed, or stored only within material access areas enclosed within a protected area. Additionally, Category I quantities of SNM shall be stored in SNM vaults equipped with Departmental-approved intrusion alarm systems or in a vault-type room so equipped, and not less than five security inspectors shall respond to a verified intrusion alarm within 5 minutes.
- b. Category I quantities of SNM shall always be under material surveillance procedures with at least two "Q"-cleared and knowledgeable authorized individuals unless it is under locked storage in a vault or vault-type room as noted in paragraph 4a, above.
- c. Any person acting alone who is in a position to steal, sabotage, divert, or conceal the diversion of Category I quantities of SNM (with appropriate consideration given to the safeguards provided the SNM), shall possess a "Q" access authorization. Uncleared persons may be permitted access to a protected area only under escort of an "S"-, "L"-, or "Q"-cleared individual and to a material access area only under escort of a "Q"-cleared person. (Note: Equivalent clearances may be used subject to management approval.)
- d. SNM facilities holding Category I quantities of SNM shall be surveyed at least annually to evaluate the adequacy of physical protection provisions. In addition, surveys should be conducted as often as is necessary to maintain a high standard of performance as determined by the responsible operations office manager. Reports of surveys

11-4-85

shall be furnished promptly to the contractor surveyed, to the Director of Safeguards and Security, and to the responsible outlay program manager.

- e. Signs prohibiting trespassing shall be posted around the perimeter of and at all entrances to the use or storage area, and reward signs and signs prohibiting the introduction of contraband articles and authorizing inspections/searches of vehicles, packages, or persons either entering or exiting shall be posted at all entrances to the use or storage areas.

5. PROTECTION OF CATEGORY I QUANTITIES OF SPECIAL NUCLEAR MATERIAL AND CLASSIFIED CONFIGURATIONS OF CATEGORY II QUANTITIES OF SPECIAL NUCLEAR MATERIAL - IN TRANSIT.

- a. Shipments of Category I quantities of SNM and classified configurations of Category II quantities of SNM shall be made by one of the following methods:

(1) Highway.

- (a) In locked and sealed safe secure trailers, towed by special tractors, accompanied by at least six Albuquerque Operations Office Transportation Safeguards Division couriers. All convoy vehicles shall be driven by Albuquerque Transportation Safeguards Division couriers.
- (b) Tractors and escort vehicles shall maintain intra-convoy communication with very high frequency radios and two-way communication with high frequency SECOM radios.
- (c) The vehicle containing the shipment shall be guarded continuously during the trip.
- (d) All shipments shall be made without intermediate stops, except for emergency reasons, driver relief, meals, refueling, or transfer of cargo.
- (e) At least one escort vehicle shall accompany each shipment.
- (f) Shipments of individual units containing Category I quantities of SNM and weighing over 5,000 pounds may be transported using conventional or flatbed trailers in accordance with a special plan approved by the Manager, Albuquerque Operations Office, or Manager, Pittsburgh Naval Reactors Office for Naval Reactors core shipments after coordination with the Office of Safeguards and Security.

- (g) Movements of Category I quantities of SNM between protected areas at the same site or between protected areas and loading areas at the same site, shall be escorted by couriers or security inspectors in a two-way radio-equipped vehicle. Such movements may be made by safe secure trailers or security-approved conventional vehicles.
- (h) Movements of Category I quantities of SNM within a protected area shall be under material surveillance procedures.
- (2) Train. Nonweapons parts weighing less than 5,000 pounds, but more than 1,000 pounds, per unit must be shipped in locked and sealed rail cars accompanied by at least three Departmental couriers. Individual units (excluding nuclear weapons or devices) weighing over 5,000 pounds can be shipped on flatcars accompanied by only one courier. Couriers accompanying train shipments shall utilize SECOM.
- (3) Air Transportation. If not otherwise prohibited by statute or implementing instructions, air shipments may take place in aircraft owned by the Department or under Departmental contract, with the material in the custody of at least two Albuquerque Transportation Safeguards Division couriers with pilot(s) and other crew members possessing "Q" access authorization. The cargo, when in their custody, shall be under the direct observation of the couriers during all land movements and loading and unloading operations.
- b. There shall be a detailed inspection/search of the transport vehicle prior to loading and shipment to assure that sabotage devices that could facilitate theft of the SNM have not been implanted or that sabotage has not been initiated, and that unauthorized persons are not aboard.
- c. Written procedures approved by the responsible operations office shall be followed by courier personnel responsible for the shipment of SNM.
- d. DOE F 1540.2, "Courier Receipt Book," or equivalent shall be executed at all points at which the SNM in transit changes custody.
- e. Shipments shall be scheduled in irregular patterns and preplanned to avoid areas or routes of high risk and areas of natural disaster or civil disorders, such as strikes or riots.
- f. Couriers shall maintain vigilance for the presence of conditions or situations which might threaten the security of the shipment, take such action as circumstances might require to avoid interference with continuous safe secure passage of the cargo vehicle, provide assistance to or summon aid for the crew of the cargo vehicle in

case of emergency, check seals or locks at each stop where time permits, and observe the cargo vehicle and adjacent areas during stops or layovers.

- g. In an emergency where SNM is transferred from one vehicle to another outside the protected areas, the Departmental courier accompanying the shipment shall keep the shipment under surveillance by observing the opening of the cargo compartment of the original vehicle and all phases of the transfer, assuring that all the material is included in the second vehicle, and checking locks and seals.
- h. When SNM is transferred from storage to a vehicle or vice-versa, at least two security inspectors or couriers shall keep the shipment under surveillance. At least two couriers shall assure that the shipment is complete by checking locks, seals, and documentation, and by witnessing the opening or closing, as appropriate, of the cargo compartment.
- i. All persons who have access to the cargo, or control over it, including drivers, loaders, and handlers must possess a "Q" access authorization or an "L," "S," or "TS" access authorization and be under the surveillance of a "Q"-cleared employee.
- j. A multilevel continuous sampling audit of all recurring shipments of significant quantities of special nuclear materials under the jurisdiction of the Albuquerque Operations Office (those occurring more than five times a year) shall be made by the Albuquerque Operations Office to assure compliance with established security standards and procedures. Multilevel continuous sampling as applicable to this requirement is described in the "DOD Inspection and Quality Control Handbook, H-106." The sampling plan in H-106 describes three levels of sampling ($f = 1/3, 1/9, 1/27$) and the criteria for changing sampling levels. During the initial period of implementing this survey concept, audits shall be performed at frequency level 2 ($1/9$) until the Manager, Albuquerque Operations Office, determines that a high performance level has been achieved in keeping with the sampling plan; then audits will occur at frequency level 3 ($1/27$). Should a major discrepancy be found at the latter audit rate, the frequency of audits will return again to level 2 until a high level performance is again achieved. The Manager, Albuquerque Operations Office, will direct an increase in audit frequency for any portion of the system whenever, in his judgment, changes in personnel, equipment, risk, or procedures so indicate. The Albuquerque Operations Office shall require approval of the Assistant Secretary for Defense Programs, or his designee, for any deviation from this sampling plan. Audit reports requiring change of frequency due to detection of a major discrepancy shall be forwarded to the designees. Significant violations of procedures by couriers shall be reported immediately to the Manager, Albuquerque Operations Office, and after evaluation to DP-34.

- k. The number of Category I shipments shall be minimized consistent with operational requirements.

6. PROTECTION OF CATEGORY II QUANTITIES OF SPECIAL NUCLEAR MATERIAL - IN USE OR STORAGE.

- a. Category II quantities of SNM shall be used, processed, and stored in a protected area. The protected area requirements may be reduced subject to detailed justification contained in the approved site-specific safeguards and security plan. No fewer than three security inspectors shall respond to verified intrusion alarms in the protected area within 10 minutes.
- b. Any person acting alone who is in a position which would permit him to divert or to conceal the diversion of Category II quantities of SNM (with appropriate consideration given to the safeguards provided the SNM) shall possess a "Q" access authorization. Uncleared persons may be permitted access to the protected area only under escort of an "S"-, "L"-, "TS"-, or "Q"-cleared individual. (Note: Equivalent clearances may be used subject to management approval.)
- c. SNM facilities holding Category II quantities of SNM shall be surveyed to evaluate the adequacy of physical protection provisions at least annually. In addition, surveys should be conducted as often as is necessary to maintain a high standard of performance as determined by the responsible field element. Reports of surveys shall be furnished to DP-34 and to the responsible outlay program manager on a timely basis.
- d. Unoccupied rooms or buildings (or a portion of a building) containing Category II quantities of in-process SNM shall be equipped with Departmental-approved intrusion alarm systems or other equally effective means. Access to such rooms shall be limited to individuals performing their official duties. Security inspector response time to alarms shall not be more than 10 minutes.
- e. Category II quantities of SNM shall be stored in vaults, vault-type rooms, or security containers which are protected with Departmental-approved intrusion alarm systems, with a security inspector response time of not more than 10 minutes.
- f. The SNM shall be in storage or under material surveillance procedures.
- g. Signs prohibiting trespassing shall be posted around the perimeter of and at all entrances to the use or storage area, and reward signs and signs prohibiting the introduction of contraband articles and authorizing inspections/searches of vehicles, packages, or persons either entering or exiting shall be posted at all entrances to the use or storage areas.

7. PROTECTION OF CATEGORY II QUANTITIES OF SPECIAL NUCLEAR MATERIAL - IN TRANSIT. (See page VI-4, paragraph 5, for in-transit protection for classified configurations of Category II quantities of SNM.)

a. Shipments of Category II quantities of SNM shall be made by one of the following methods:

(1) Truck.

- (a) Category II quantities of SNM may be shipped by Government-owned or exclusive-use truck by commercial carrier in the custody of at least two escorts, at least one of whom possesses a "Q" access authorization, with the other possessing an "L" access authorization or equivalent.
- (b) Cargo compartments of the trucks shall be locked and sealed.
- (c) Escorts shall maintain frequent periodic communication with a control station which can request appropriate law enforcement agency response.
- (d) Escorts shall maintain the shipment under surveillance during the trip.
- (e) All shipments shall be made without any intermediate stops except for emergency reasons, driver relief, meals, refueling, or to transfer cargo.
- (f) There shall be a detailed inspection/search of the transport vehicle prior to loading and shipment to assure that sabotage devices have not been implanted or that sabotage has not been initiated and that unauthorized persons are not aboard.

(2) Train.

- (a) Category II quantities of SNM may be shipped by train in the custody of at least two escorts, at least one of whom possesses a "Q" access authorization, with the other possessing an "L" access authorization, or equivalent.
- (b) Cargo compartments shall be locked and sealed.
- (c) Escorts shall maintain frequent periodic communication with a control station which can request appropriate law enforcement agency response.
- (d) Escorts shall maintain the shipment under surveillance during the trip.

- (e) There shall be a detailed search of the transport vehicle prior to loading and shipment to assure that sabotage has not been initiated and that unauthorized persons are not aboard.
- (3) Air Transportation. If not otherwise prohibited by statute or implementing instructions, air shipments of Category II quantities of SNM may take place. The material must be attended by at least two escorts, at least one of whom possesses a "Q" access authorization with the other possessing an "L" access authorization or equivalent. The shipments must be under the direct observation of the escorts during all land movements and loading and unloading operations.
- b. Procedures approved by the responsible operations office managers shall be followed by all personnel associated with the shipment.
- c. DOE F 1540.2, or equivalent, shall be executed at all points where the in-transit SNM changes custody.
- d. Route choice and schedule should be based on consideration to avoid areas of natural disasters or civil disorders and to provide the minimum number of cargo transfers and minimum length of transit time.
- e. Movements of Category II quantities of SNM within a protected area shall be under material surveillance procedures.
- f. Movements of Category II quantities of SNM between protected areas at the same site shall be under escort by at least one security inspector.
- g. Escorts shall maintain continued vigilance for the presence of conditions or situations which might threaten the security of the shipment, take appropriate action to avoid interference with continuous safe passage of the cargo vehicle, provide assistance to or summon aid for the crew of the cargo vehicle in case of emergency, check seals or locks at each stop where time permits, and observe the cargo vehicle and adjacent areas during stops or layovers.
- h. In an emergency, where SNM is transferred from one vehicle to another, at least two escorts, at least one of whom possesses a "Q" access authorization, with the other possessing an "L" access authorization or equivalent, shall keep the shipment under surveillance by observing all phases of the transfer, assuring that all the material is included in the second vehicle, and checking locks and seals.

- i. Significant violations of procedures shall be reported immediately to the responsible field element which shall, after making an evaluation, forward a written report to DP-34.
 - j. Office of Safeguards and Security Field Elements shall conduct transportation security surveys of carriers at least annually. Surveys shall be coordinated with the cognizant field transportation office.
 - k. The number of Category II shipments shall be minimized consistent with operational requirements. When feasible, separate shipments of Category II SNM should be combined into a single shipment and, if Category I quantities are present in the combined shipment, sent under the requirements on page VI-4, paragraph 5.
8. PROTECTION OF CATEGORY III QUANTITIES OF SPECIAL NUCLEAR MATERIAL - IN USE OR STORAGE.
- a. Category III-A Quantities of Special Nuclear Material.
 - (1) When unattended, Category III-A quantities of SNM shall be secured within a locked Departmental-approved security container or within a locked room.
 - (2) When unattended, the container or locked room containing the material shall be under the protection of a Departmental-approved intrusion detection alarm system, or patrolled at intervals not to exceed 2 hours, or located in a protected area.
 - (3) Access to the material shall be limited to properly cleared employees in positions which have been specifically designated by management as requiring access to Category III-A quantities of SNM in the course of assigned duties and to authorized visitors who are under continuous escort of employees in such designated positions.
 - (4) Protective force response to alarms shall be not more than 10 minutes.
 - (5) Packages, briefcases and similar handcarried items, and all vehicles shall be subject to inspection/search by the individual controlling access to the use or storage area or to the protected area, if applicable. The inspection/search on entering shall be made to assure that explosives or other contraband are not introduced. Personnel and packages shall be subject to inspection/search upon leaving the use or storage area to assure that SNM is not being surreptitiously removed.

- (6) Signs prohibiting trespassing shall be posted around the perimeter of and at all entrances to the use or storage area, and reward signs and signs prohibiting the introduction of contraband articles and authorizing inspections/searches of vehicles, packages, or persons either entering or exiting shall be posted at all entrances to the use or storage areas.
 - (7) SNM facilities holding Category III-A quantities of SNM shall be surveyed to evaluate the adequacy of safeguards and security provisions at least every 2 years. Reports of inspections shall be furnished to DP-34 and appropriate outlay program managers.
 - b. Category III-B Quantities of Special Nuclear Material shall be received, used, processed, and stored in accordance with operations office-approved safeguards and security plans.
9. PROTECTION OF CATEGORY III QUANTITIES OF SPECIAL NUCLEAR MATERIAL - IN TRANSIT.
- a. Shipments of all Category III quantities of SNM may be made by one of the following methods: truck, rail, air, or water in commercial, for-hire vehicles. (If not otherwise prohibited by statute or implementing instructions, air shipments of Category III quantities of SNM may take place.)
 - b. Packages shall be sealed.
 - c. Shipments, excepting shipments of laboratory analysis samples, shall be made under arrangements which provide the capability to trace and identify, within 24 hours of request, the precise leg of a journey where a shipment went astray in the event of its nonarrival at destination within the prescribed timeframe.
 - d. Advance notification of the estimated time of arrival to be received prior to dispatch, with written confirmation following not later than 48 hours after dispatch, shall be provided by the shipper to the consignee.
 - e. The consignee shall promptly notify the shipper by telephone upon determination that a shipment has not arrived within a reasonable time and shall provide written confirmation of such notification.
 - f. In the event that an exclusive-use vehicle is required for other than safeguards and security reasons, the following provisions apply:
 - (1) The vehicle shall be given a detailed search prior to loading of shipment to assure that sabotage devices have not been implanted or that sabotage has not been initiated; and

- (2) The vehicle shall be sealed and all seal numbers noted on the shipping papers.
- g. Shipments shall be made in accordance with all applicable Federal regulations.
- h. The number of Category III shipments shall be minimized consistent with operational requirements. When feasible, separate shipments of Category III SNM should be combined into a single shipment and, if Category II or I quantities are present in the combined shipment, sent under the requirements on pages VI-4 and VI-8, paragraphs 5 or 7, respectively.

PHYSICAL PROTECTION
CATEGORIZATION OF NUCLEAR MATERIAL

Special Nuclear Material	Category ^{1/} I	Category ^{1/} II	Category ^{2/} III-A	Category III-B
Plutonium	2 kg or more	400-1,999 grams	220-399 grams	1-219 grams
Uranium-233	2 kg or more	400-1,999 grams	220-399 grams	1-219 grams
Uranium-235 (Contained in Uranium enriched to 20% or more)	5 kg or more	1,000- 4,999 grams	350-999 grams	1-349 grams
Uranium-235 (Con- tained in Uranium enriched to less than 20%)	-	-	-	All quantities one gram or more.

1/ If Plutonium or Uranium-233 is combined with Uranium-235, the amounts of Plutonium or Uranium-233 shall be multiplied by 2.5 to arrive at the limits shown.

2/ A Plutonium and/or Uranium-233 content of less than 400 grams may be combined with Uranium-235 when the total content is less than 1,000 grams.

CHAPTER VII

PHYSICAL PROTECTION OF DEPARTMENTAL PROPERTY AND FACILITIES

1. BASIC CONSIDERATIONS. Property protection areas should be established to protect against damage or destruction arising from deliberate acts of arson, civil disorder, riot, sabotage, terrorism, or vandalism and to deter and prevent the theft of Government property at facilities. The measures taken shall be adequate to give reasonable assurance of protection and may include physical barriers, security inspectors or guards, intrusion alarm systems, locks and keys, or security areas.
2. STANDARDS AND REQUIREMENTS.
 - a. Physical Barriers. Barriers such as walls or fences are intended to control or impede access. Walls of buildings normally constitute an adequate physical barrier.
 - b. Security Inspectors or Guards.
 - (1) Protection may be provided by security inspectors or guards as deemed appropriate by the Head of the Field Element or, for Headquarters, by DP-34.
 - (2) Security inspectors or guards should make patrols at irregular intervals, but not less frequently than once every 8 hours during nonworking periods. Where arrangements can be made with local police forces to conduct patrols, guard or custodian patrols need not be provided.
 - c. Intrusion Alarm Systems. Intrusion alarm systems may be used to provide positive notification of penetration into a Departmental facility or onto its premises. An intrusion alarm system is considered to be of significant value when a response time not exceeding 15 minutes is assured and when the system itself is dependable.
 - d. Locks and Keys. Key locks in doors should be resistant to picking and jimmying, and combination locks should be resistant to manipulation. Padlocks should be of sturdy construction and resistant to opening by picking, rapping, forcing, or the use of shims or similar techniques. A system of accountability and positive controls for keys and combinations should be in place. When a key is unaccounted for, the lock(s) which it opens should be replaced immediately. Combinations should be changed when a person having access thereto is terminated or permanently assigned outside the function involved.
 - e. Property Protection. Where practical, property protection facilities shall include property protection areas as defined in Chapter II of this Order. In cases where, because of facility size or nature, this is impractical, an area encompassed by physical barriers and subject to

access controls shall be established as deemed necessary by the respective Head of the Field Element in coordination with the Office of Procurement Operations (MA-45) and with DP-34.

- f. Access. Access to a Departmental facility during working hours shall be controlled by receptionists or by employees who have been assigned specific responsibility for assuring that only persons with proper authorization are admitted. When unoccupied, such facilities shall be locked with approved locking devices and shall be protected by such other means as the Head of the Field Element or, for Headquarters, DP-34, deems appropriate.
- g. Prohibited Articles. Firearms, explosives, incendiary devices, and similar articles shall not be taken into Departmental facilities without proper authorization. As a condition of access, vehicles and handcarried items of persons entering Departmental facilities shall be subject to inspection/search to ascertain that they do not contain such prohibited articles. Where the Head of the Field Element or, for Headquarters, DP-34, decides that vehicles and handcarried items shall be subject to inspection/search, a statement to this effect and a list of prohibited articles shall be posted conspicuously at each entrance to a Departmental facility.
- h. Searches of Vehicles and Handcarried Items. Vehicles, packages, briefcases, lunch boxes, and other handcarried items shall be subject to inspection/search upon leaving a Departmental facility that is subject to the physical protection requirements of this Order to assure that they do not contain Government property which is being removed without proper authorization.
- i. Posting Against Trespassing. "No Trespassing" posting of Departmental property pursuant to section 229, Atomic Energy Act of 1954, as amended, shall be handled in accordance with the Responsibilities and Authorities as set forth on pages 1 through 10, paragraph 7.
- j. Emergency Plans. Emergency plans shall be established and integrated into existing Departmental emergency plans.
- k. Physical Protection Surveys. A survey and report should be made of each physical protection facility at least once every 24 months. A report of findings shall be made on a timely basis and copies of the report shall be submitted to DP-34, IG-1, the responsible field element, and to the appropriate Headquarters program office.
- l. Incident Reports. Reports of incidents shall be made in accordance with the provisions of DOE 5633.1.

CHAPTER VIII

TRESPASSING ON DEPARTMENTAL PROPERTY

1. STATUTORY PROVISIONS. Section 229 of the Atomic Energy Act of 1954, as amended, prohibits unauthorized entry and unauthorized 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 subject to the jurisdiction, administration, or in the custody of the Department. The statute provides for posting of regulations and penalties for violations.
2. CRITERIA. Selection of facilities, installations, and real property for posting generally will be based upon the need for supplementing other Federal statutes protecting against espionage, sabotage, or depredation of Government property. Real property may be posted for protection for nonsecurity reasons if deemed necessary.
3. PROPOSALS.
 - a. Conditions. Proposals for the posting of facilities, installations, or real property, or amendment to or revocation of a previous proposal will be submitted if:
 - (1) The property is owned by, or contracted to, the United States for use by the Department;
 - (2) The property requires protection under section 229, Atomic Energy Act of 1954, as amended; and
 - (3) A previous notice needs to be amended or revoked.
 - b. Contents.
 - (1) 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 which can be physically delineated by the posting indicated in paragraph 4, below.
 - (2) 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.

4. POSTING REQUIREMENTS.

- a. Upon approval of DP-1, the 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 in accordance with the requirements set forth in paragraph 4b, below.
- b. Property approved by DP-1 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 as to provide reasonable assurance of notice to persons who enter therein, with signs measuring at least 11 inches by 14 inches and reading as appears on Attachment VIII-1. The "No Trespassing" signs presently in use contain language which refers to the "Energy Research and Development Administration." These signs are acceptable for continued use until such time that it is considered practical to replace them, using the language as stated in Attachment VIII-1.

5. NOTIFICATION TO THE FEDERAL BUREAU OF INVESTIGATION. Notification of the date of posting, relocation, or removal of posting, or other change and the identity of the property involved, shall be furnished promptly to the local office of the Federal Bureau of Investigation exercising investigative responsibility over the property.6. VIOLATIONS. Violations of the prohibitions as posted shall be reported in accordance with the provisions of DOE 5633.1.

EXAMPLE OF A "NO TRESPASSING" SIGN FOR A DEPARTMENT OF ENERGY FACILITY

NO TRESPASSING

BY ORDER OF

THE UNITED STATES

DEPARTMENT OF ENERGY

The unauthorized entry upon any facility, installation, or real property subject to the jurisdiction, administration, or in the custody of the Department of Energy, which has been designated as subject to the provisions contained in 10 CFR part 860 of the rules and regulations of the Department of Energy, is prohibited, and the unauthorized 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 facility, installation, or real property is prohibited.

Whoever willfully violates the aforesaid regulation shall, upon conviction thereof, be punishable by a fine of not more than \$1,000. Whoever willfully violates this regulation with respect to any facility, installation, or real property enclosed by a fence, wall, floor, roof, or other structural barrier, shall be guilty of a misdemeanor and, upon conviction thereof, shall be punished by a fine not to exceed \$5,000 or imprisonment for not more than 1 year, or both.

By authority of section 229 of the Atomic Energy Act of 1954, as amended, and 10 CFR part 860 of the rules and regulations of the Department of Energy, this facility, installation, or real property has been designated as subject to these regulations by the United States Department of Energy.

CHAPTER IX

PHYSICAL PROTECTION OF DEPARTMENTAL NUCLEAR REACTORS

1. POLICY AND OBJECTIVES. It is Departmental policy to physically protect all SNM and key facilities, including nuclear reactors, against acts of sabotage. The objectives of this policy are to:
 - a. Protect the health and safety of the public; and
 - b. Maintain program continuity by preventing an unacceptable interruption of facility operations.
2. GENERAL. Physical protection systems for Departmental nuclear reactors should be designed and implemented to counter a range of threats, including a group of several well-armed, trained, and dedicated saboteurs with or without the assistance of a single, well-placed insider. The group may operate in several modes, including frontal and diversionary assault modes, or by a combination of assault, stealth, and deceit. Additional credible threats which the physical protection system should counter include intrusion by organized demonstrators and individual vandals.
3. PROCEDURES AND REQUIREMENTS.
 - a. Security Perimeters. Each reactor shall be contained within a concentric set of security perimeters, with the innermost being the vital area perimeter. Next, outboard will be the protection area perimeter(s), and, finally, the isolation zone. Specific requirements are:
 - (1) Vital Area. Vital areas contain all vital equipment within their perimeters. There may be more than one vital area within a given protected area. The perimeter of a vital area shall be established to permit detection of unauthorized attempts at entry. Access controls shall be provided: (a) for annunciation and assessment of an alarm at a central guardpost, and (b) to delay an adversary from gaining access to vital equipment until the arrival on scene of response forces. Alternately, vital areas shall be contained in protected areas which meet these requirements.
 - (2) Protected Area. As defined in this Order (see Attachment 2, page 6, paragraph 39).
 - (3) Isolation Zone. As defined in this Order (see Attachment 2, page 5, paragraph 26).

b. Access Controls.

- (1) All persons admitted to protected or vital areas must be properly cleared and authorized, or be under the escort of a cleared and authorized person knowledgeable of facility operations, safeguards, and security procedures.
- (2) All persons who are afforded unescorted access to protected areas will possess at least an "L" or "S" clearance.
- (3) All persons who are afforded unescorted access to vital areas will possess at least a "Q" or "TS" clearance.

c. Records. Records must be maintained of all nonroutine personnel entering a protected area or vital area.d. Onsite Security Force. The onsite security force will have the capability of either defeating or delaying, until sufficient backup units arrive, the threat as detailed in the generic threat guidance issued by DP-1 and as stated in the site-specific safeguards and security plan. In no event should there be fewer than five security inspectors available for response within 5 minutes of an alarm. These responding security inspectors shall be other than those manning the site's central alarm assessment and control center.

