

U.S. Department of Energy
Washington, D.C.

ORDER

DOE 5632.1A

2-9-88

SUBJECT: PROTECTION PROGRAM OPERATIONS

1. PURPOSE. To establish Department of Energy (DOE) policies for the physical protection of security interests and baseline physical protection standards.
2. CANCELLATION. DOE 5632.4, PHYSICAL PROTECTION OF SECURITY INTERESTS, of 11-4-85, and DOE 5631.3, ISSUANCE AND CONTROL OF CREDENTIALS, SHIELDS, AND COURIER CARDS, of 2-3-87.
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. BACKGROUND.
 - a. Physical protection of security interests encompasses three major activities: physical security systems, protective forces, and system performance tests. It covers the entire physical security program at a facility including security equipment, procedures, protective forces, management and supervision, and the integration of these elements into a total physical protection security system.
 - b. This Order establishes the authorities and responsibilities for managing and implementing the protection of security interests and sets forth the framework for the following 5632 Order series which defines the policies and baseline requirements specific to related aspects of protection program operation:
 - (1) Physical Protection of Special Nuclear and Vital Equipment;
 - (2) Physical Protection of Classified Matter;
 - (3) Physical Protection of Departmental Property and Unclassified Facilities;
 - (4) Protective Forces;

DISTRIBUTION:
All Departmental Elements

INITIATED BY:
Office of Safeguards and
and Security

- (5) Protection Program Operations - Systems Performance Tests; and
 - (6) Issuance, Control, and Use of Badges, Passes, and Credentials.
- c. The standards set forth in the DOE Standards and Criteria have their foundation in DOE Orders which contain the policy for developing a safeguards and security program. These standards are supported by criteria which are examples of some of the mechanisms available for use by management in appropriately implementing the policy. The Protection Program Operations section of the DOE Safeguards and Security Standards and Criteria provides information and guidance for operation of an effective protection program. The Standards and Criteria shall be considered when designing, modifying, or operating DOE facilities. Standards and Criteria applicable to each facility shall be identified on a site-specific basis and modified, as appropriate, to address site-specific needs. Protection programs must be designed to address site-specific characteristics.
- d. The classified generic threat guidance issued by the Assistant Secretary for Defense Programs (DP-1) must be considered in the design and implementation of protection programs.
5. POLICY. The Department's security interests are to be protected from theft or diversion of special nuclear material (SNM), industrial sabotage, radiological sabotage (e.g., induced criticality), espionage, loss or theft of classified matter or Government property, and other hostile acts which may cause unacceptable adverse impacts on national security or on the health and safety of the public. Specific policies and objectives, as identified in this Order series, are expressed in terms of what is required. 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 and the health and safety of the public. The protection provided Departmental security interests shall be comparable to that provided by other Government agencies with similar security interests.
6. CONCEPT OF OPERATIONS.
- a. DOE's policy for protecting security interests applies equally to all Departmental Elements. However, this policy is implemented at a wide range of facilities; site-specific characteristics must be considered to assure that Departmental security interests are provided appropriate and cost-effective protection. In order to allow for effective protection, programs shall be designed to address site-specific requirements.

- b. When it is impractical or not cost-effective to meet a specific requirement of this Order series, alternate means of providing adequate protection may be proposed. There are two categories of exceptions involving the following:
 - (1) Security of Category I and II quantities of SNM and/or materials, facilities, or operations covered by the classified threat guidance issued by DP-1. These exceptions shall be developed and approved by the Heads of Field Elements and submitted in writing to the Director of Safeguards and Security (DP-34) for review and concurrence prior to implementation. Written records of such exceptions shall be included in the appropriate site-specific safeguards and security plan(s) and/or Master Safeguards and Security Agreements (MSSAs).
 - (2) 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 shall be approved by the Head of Field Elements and included in the appropriate site-specific safeguards and security plan(s) and/or MSSAs.
- c. MSSAs are the preferred mechanism for implementing DOE policy and defining appropriate protection levels and strategies for particular security interests on a site-specific basis that are consistent with the operational requirements, the applicable threat, the target attractiveness, and the potential risks. The MSSA process is also an appropriate mechanism for identifying, justifying, and documenting site-specific protection systems or procedures that do not conform with the baseline requirements of this Order series.
- d. Site-specific protection programs shall be documented in appropriate safeguards and security plans and/or MSSAs which shall specifically identify and justify deviations from the basic requirements of this Order series.
- e. Implementation of emergency management/preparedness elements of this Order shall be in accordance with DOE 5500.1A, EMERGENCY MANAGEMENT SYSTEMS, and subsequent issuances of the 5500 series Orders.
- f. For all facilities having MSSAs, evaluations, inspections, appraisals, and audits shall be formulated utilizing the MSSAs as the basis for developing the requirements.

- g. Safeguards and security protective measures will be developed and implemented to assure balance of the impact on safety requirements.

7. REFERENCES. See Attachment 1.

8. DEFINITIONS. See Attachment 2.

9. RESPONSIBILITIES AND AUTHORITIES.

- a. The Secretary has overall responsibility and authority for DOE programs and takes necessary management actions, through the Under Secretary, to ensure that the Department's safeguards and security (S&S) interests are effectively protected.

- b. Program Secretarial Officers (PSO) have primary responsibility to ensure that S&S interests under their jurisdiction are protected in accordance with Departmental requirements. Program Secretarial Officers shall:

- (1) Require the preparation of site-specific safeguards and security plans and MSSAs, where appropriate, for interests over which they have programmatic responsibility and maintain oversight on the development of such plans in coordination with cognizant operations offices and DP-34.
- (2) Require that appropriate 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.
- (3) Perform reviews to evaluate safeguards and security program funding of activities under their programmatic jurisdiction.
- (4) Participate in the development, review, and concurrence of Orders and standards for the safeguards and security interests associated with the programs under their cognizance.
- (5) Consult DP-34 regarding all aspects of security operations for Headquarters-administered contracts.
- (6) 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, their contractors or subcontractors; and to foreign governments under agreements for cooperation.

- (7) Obtain the Assistant Secretary for Management and Administration (MA-1) support and guidance on the policy and procedures for the administration of the planning, design, and construction or alternation of facilities having a security interest.
- c. Assistant Secretary for Defense Programs (DP-1) provides management direction and coordination in the development, implementation, and oversight of the comprehensive Departmental safeguards and security program based on applicable Departmental directives. DP-1 shall:
- (1) Ensure adequate resources to support the Department's Safeguards and security program are provided.
 - (2) Authorize security shipments outside the United States, other than those consigned to nuclear explosive test sites, after the Director of Safeguards and Security advises as to the adequacy of security measures to protect such shipments.
 - (3) Authorize, through the Deputy Assistant Secretary for Military Application (DP-20), the transmission of classified 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) Approve, 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 authorize for publication in the Federal Register a listing of the properties and facilities designated for "No Trespassing" notice.
 - (5) Implement the information collection and clearance requirements contained in Title 5 CFR Part 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.
- d. Director of Safeguards and Security.
- (1) Develops standards and criteria for the physical protection of Departmental security interests, with the concurrence of responsible Departmental Elements.

- (2) Clarifies DOE safeguards and security Orders in a timely manner and disseminates appropriate clarifications, in writing, to the Heads of Departmental Elements, as appropriate, and prepares and distributes a report summarizing any recent clarifications.
- (3) Clarifies, modifies or interprets the standards and criteria. Modifies, as appropriate, and reissues the standards and criteria document annually or as-needed.
- (4) Establishes and maintains a system to tie safeguards and security objectives to overall Departmental plans and programs.
- (5) Provides staff assistance to Departmental Elements in the development of safeguards and security plans and in the implementation of physical protection systems.
- (6) Reviews safeguards and security plans and Master Safeguards and Security Agreements, as appropriate, and provides comments to the responsible Program Secretarial Officers and Heads of Field Elements.
- (7) Reviews and provides concurrence to Heads of Field Elements on exceptions to the provisions of physical protection Orders 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. (Note: Exceptions made by the field on an emergency basis may be implemented on a temporary basis prior to review and concurrence by DP-34.)
- (8) Maintains a master facility register of all DOE facilities and interests approved by DOE for physical protection under the requirements of this Order.
- (9) Monitors the execution of physical protection surveys of property and facilities under the jurisdiction of field elements.
- (10) Determines that corrective measures are being planned and/or implemented to address findings identified in survey and inspection reports; consults with the cognizant Program Secretarial Officers and field element managers to assure that cost-effective corrective measures are planned and implemented to meet any deficiencies identified.
- (11) 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.
- (12) Reviews and coordinates the development of technology to protect nuclear explosives, their components, and SNM in transit.

- (13) Develops and assures, in coordination with Program Secretarial Officers, implementation of procedures governing security requirements for Headquarters operations.
- (14) Conducts surveys of the facilities under Headquarters cognizance in accordance with DOE 5634 1A, SECURITY SURVEYS, NUCLEAR MATERIAL SURVEYS, AND FACILITY APPROVAL.
- (15) 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 regarding the evaluation.
- (16) Maintains liaison with the Federal Bureau of Investigation (FBI) and other Federal law enforcement and security agencies with respect to matters of physical protection policy and tactical situations at Headquarters or in support of field element requests.
- (17) 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.
- (18) Recommends to DP-1 for approval and subsequent publication in the Federal Register a listing of property and facilities designated for "No Trespassing" posted under section 229, Atomic Energy Act of 1954, as amended.
- (19) Procures and distributes inserts for identification badges (DOE F 5631.19) to field elements. (Only issues badges.)
 - (a) Issues employee identification badges to Headquarters employees and security credentials to appropriate Headquarters and field element personnel.
 - (b) Maintains records of such badges for Headquarters employees.
- (20) Disseminates reports of losses and recoveries of employee identification badges.
- (21) Oversees and administers the design, issuance, and control of all DOE credentials except for the Deputy Assistant Secretary for Intelligence (DP-40) and the Inspector General (IG-1), who administer the design, issuance, and control of DOE credentials to persons under their cognizance.

- (22) Provides Departmental Elements with the necessary inventories of credentials for local issuance.
- (23) Maintains a central accountability record of all credentials.
- (24) Maintains central records for inventories of unused, lost, stolen, and/or destroyed credentials.
- (25) Establishes Departmental policies and procedures regarding the issuance of credentials.
- (26) Reviews, on an as-needed basis, Departmental policies and requirements to assure that protection afforded DOE security interests is comparable to that required by other Government agencies with similar security interests.
- (27) Coordinates with EH-1 and field elements, as appropriate, to assure that emerging safeguards and security systems and requirements will have minimum adverse effects on safety.

e. Deputy Assistant Secretary for Military Application.

- (1) Administers the transportation safeguards system for domestic shipments of nuclear explosives, Category I and II quantities of SNM (excluding naval reactor core shipments), and other cargos deemed appropriate and agreed to by the Manager, Albuquerque Operations Office, and respective Heads of Departmental Elements. (Naval reactor core shipment program responsibility rests with the Deputy Assistant Secretary for Naval Reactors.)
- (2) Develops and implements 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 and administers the program for the control of Weapon Data.

f. Assistant Secretary, Management and Administration, through the Director of Project and Facilities Management.

- (1) Develops and maintains general design criteria for application in the planning, design, and construction or alteration of facilities and incorporates guidance for physical protection of security facilities 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.

g. Assistant Secretary for Environment, Safety, and Health.

- (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.
- (5) Provides consultation to help assure that development and implementation of Safeguards and Security measures achieve consistency with safety requirements.

h. The Director, Office of Security Evaluations provides, for DP-1, oversight of the implementation of all safeguards and security policies and programs for all facilities under Departmental cognizance.

i. Deputy Assistant Secretary for Naval Reactors.

- (1) Administers the Naval Nuclear Propulsion Program, including oversight of program support for security activities of Headquarters, the Pittsburgh Naval Reactors Office, Schenectady Naval Reactors Office, together with Naval Reactors prototype sites (Kesselring, Windsor, and Naval Reactors Facility).
- (2) Requests assistance from Defense Programs and appropriate field element activities as necessary to assure that the requirements of this Order are met.
- (3) Administers the Naval reactor core shipment program.

- j. Heads of Field Elements are responsible for assuring that all operations under their jurisdiction are carried out consistent with sound safeguards and security practices and in accordance with applicable Orders. In carrying out this responsibility Heads of Field Elements shall:
- (1) Participate in the development, review, and concurrence of Orders and policy standards for safeguards and security and other security interests under their jurisdiction.
 - (2) Obtain from Deputy Assistant Secretary for Military Applications, DP-20, approval for the transmission of classified Weapon Data to the DOD, its military components, and its contractors and subcontractors.
 - (3) 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.
 - (4) 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.
 - (5) Coordinate security shipments with other Heads of Field Elements.
 - (6) Approve, as appropriate, manuals and instructions prepared by contractors or subcontractors to implement the provisions of DOE Orders.
 - (7) Develop an alternate approach to providing equivalent levels of physical protection when site or program considerations make the strict implementation of this Order infeasible. Exceptions concerning the physical protection of Category I and II quantities of SNM and/or materials, facilities, or operations covered by the classified threat guidance issued by DP-1 shall be submitted to DP-34 for review and concurrence prior to implementation. All other exceptions to the requirements of this Order may be implemented with the approval of the Heads of Field Elements.
 - (8) Issue employee identification badges and maintain records of all such badges.
 - (9) Report losses and recoveries of identification badges promptly to DP-34.
 - (10) Approve the holding of classified conferences outside approved security areas.

- (11) Plan for funding and staffing to implement Departmental protection programs, including the preparation and approval of appropriate site-specific safeguards and security plans for each Class A, B, or C facility and field elements. These plans will be furnished to the program offices involved.
- (12) 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.
- (13) 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 series and also in separate, classified guidance issued periodically by DP-1.
- (14) 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 safeguards and security of security interests under their respective jurisdictions.
- (15) 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.
- (16) Assure that "No Trespassing" notices are posted.
- (17) Ensure that employees are made fully aware of and understand their responsibilities for protecting security interests.
- (18) Approve the transmittal of classified nonnuclear matter and classified documents and information, except Weapon Data, to the DOD and its military components and to other Government agencies and to their contractors or subcontractors.
- (19) Determine which by-products of source materials or special nuclear materials may be designated as scrap (recoverable) or waste (not recoverable) for physical protection purposes.
- (20) Report immediately to the Headquarters Emergency Operations Center, in accordance with the applicable DOE 5500 series Order, any information related to an actual, attempted, or suspected act of theft, sabotage, espionage, or other hostile act

involving security interests, including losses of SNM or classified matter, or other circumstances indicating violation of Federal law.

- (21) Consult with DP-34 on questions concerning safeguards and security requirements and other matters pertaining to physical protection.
- (22) Determine annually that each security inspector and guard meets the physical and medical qualifications of Title 10 CFR 1046.
- (23) Prepare reports on expenditures for safeguards and security activities and provide copies of these reports to DP-34 and outlay program managers.
- (24) 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.
- (25) Conduct surveys of the facilities under their cognizance in accordance with DOE 5634.1A.
- (26) Request MA-1 to provide support and guidance on the policy and procedures for administration of the planning, design, construction, or alteration of facilities.
- (27) Report within 24 hours to the Headquarters Emergency Operations Center serious or major incidents involving the use of firearms, including accidental discharge, or any serious incident involving an arrest or detention.
- (28) Report, in accordance with DOE 5000.3, all discharges of firearms and other weapons other than those normally expected during training exercises.
- (29) Ensure that all appropriate safeguards and security plans, MSSAs, and implementing procedures are coordinated and appropriately integrated with DOE 5500 series to assure proper response to emergencies created by malevolent threats or acts.
- (30) Ensure that the request for, and issuance of, credentials is restricted to security personnel who require credentials in the performance of official duties.
- (31) Maintain accurate up-to-date records which reflect the disposition of all credentials to include those issued, lost, destroyed, and in stock.

- (32) Report to DP-34, in writing, any actual or alleged incident or misuse of a credential.
- (33) Retrieve and/or destroy credentials issued to persons who are:
 - (a) Terminating DOE employment;
 - (b) On extended separation from employment (i.e., excess of 90 days);
 - (c) No longer in need of a credential in the performance of official duties; or
 - (d) Being processed under Title 10 CFR Part 710 and have had their DOE access authorization suspended.
- k. Managers of the Albuquerque, Nevada, Oak Ridge, San Francisco, and Savannah River Operation Offices. In addition to the responsibilities outlined in paragraph 9i 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 concurrence by DP-1 through DP-20.
- l. Manager, Albuquerque Operations Office.
 - (1) In addition to the responsibilities outlined in paragraphs 9j and k, manages the transportation safeguards system for domestic shipment of nuclear explosives, Category I or II quantities of SNM (excluding naval reactor core shipments), and other cargos deemed appropriate and agreed to by the Manager, Albuquerque Operations Office, and respective Heads of Departmental Elements. (Naval reactor core shipment responsibility rests with the Deputy Assistant Secretary for Naval Reactors.)
 - (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.

m. Manager, Nevada Operations Office.

- (1) In addition to the responsibilities outlined in paragraphs 9j and k, 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) Approves the release of security shipments involving nuclear test devices between the Department and domestic military installations.

n. Manager, Oak Ridge Operations Office.

- (1) In addition to the responsibilities outlined in paragraphs 9j and k, provides support services and advice to the Office of Scientific and Technical Information (MA-28) in physical communications, personnel, and automated data processing security.
- (2) Determines those portions of the DOE Protection Program, as defined in the 5632 series of Orders, Title 10 CFR Parts 1046 and 1047, which apply to the Strategic Petroleum Reserve Office and its protection force officers, and implements those portions through the Contractor Officer.

BY ORDER OF THE SECRETARY OF ENERGY:



LAWRENCE F. DAVENPORT
Assistant Secretary
Management and 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 weapon, 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 1324.2, RECORDS DISPOSITION, of 5-28-80, which assigns responsibilities for the disposition of Departmental records.
3. DOE 4300.1B, REAL PROPERTY AND SITE DEVELOPMENT PLANNING, of 7-1-87, which establishes Departmental policies and procedures for planning the development and use of sites and facilities.
4. DOE 4300.2A, NON-DEPARTMENT OF ENERGY FUNDED WORK, of 12-19-86, which provides policies for work performed by agencies not funded by the Department of Energy.
5. 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.
6. DOE 5300.1 TELECOMMUNICATIONS, of 11-16-81, which establishes policy for providing telecommunications services throughout the Department.

7. 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.
8. DOE 5300.3B, TELECOMMUNICATIONS: COMMUNICATIONS SECURITY, of 2-12-87, which establishes policy for communications security for Departmental telecommunications.
9. 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.
10. DOE 5500.1A, EMERGENCY MANAGEMENT SYSTEMS, of 2-26-87, which provides policy and procedures for emergency management.
11. 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.
12. DOE 5630.13, MASTER SAFEGUARDS AND SECURITY AGREEMENT, of 2-3-88, which establishes Departmental policy for developing master safeguards and security agreements.
13. DOE 5631.5, VIOLATIONS OF LAWS, LOSSES, AND INCIDENTS OF INTERNAL SECURITY INTERESTS, of 2-12-88, which establishes Departmental procedures for follow-up action to violations of Federal laws, losses of security interest, and incidents of internal security.
14. DOE 5631.2B, PERSONNEL SECURITY PROGRAM, of 5-18-88, which establishes policies, responsibilities, and authorities for implementing the Departmental personnel security program.
15. DOE 5632.2A, PHYSICAL PROTECTION OF SPECIAL NUCLEAR MATERIAL AND VITAL EQUIPMENT, of 2-9-88, which establishes Departmental policy for the physical protection of special nuclear materials.
16. DOE 5632.5, PHYSICAL PROTECTION OF CLASSIFIED MATTER, of 2-3-88, which establishes Departmental policy for the physical protection of classified matter.
17. DOE 5632.6, PHYSICAL PROTECTION OF DOE PROPERTY AND UNCLASSIFIED FACILITIES, of 2-9-88, which establishes Departmental policy for the physical protection of DOE property and unclassified facilities.

18. DOE 5632.7, PROTECTIVE FORCES, of 2-9-88, which prescribes Departmental policy for the management, operation, and training of protective forces responsible for protecting security interests at DOE facilities.
19. DOE 5632.8, PROTECTION PROGRAM OPERATIONS: SYSTEM PERFORMANCE TESTS, of 2-4-88, which establishes Departmental policy for testing protection system capabilities.
20. DOE 5632.9, ISSUANCE, CONTROL, and USE OF BADGES, PASSES, AND CREDENTIALS, of 2-3-88, which establishes Departmental policies for the issuance, control, and use of badges.
21. DOE 5633.3, CONTROL AND ACCOUNTABILITY OF NUCLEAR MATERIALS, of 2-3-88, which prescribes Departmental policies and responsibilities for control and accountability of nuclear materials.
22. DOE 5634.1A, SECURITY SURVEYS, NUCLEAR MATERIALS SURVEYS, AND FACILITY APPROVAL, of 2-3-88, which establishes Departmental requirements for on-site security of nuclear materials surveys.
23. DOE 5635.1A, CONTROL OF CLASSIFIED DOCUMENTS AND INFORMATION, of 2-12-88, which provides guidance relative to the safeguarding and control of classified documents and information.
24. DOE 5636.3A, TECHNICAL SURVEILLANCE COUNTERMEASURES PROGRAM, of 2-3-88, which establishes the Department's Technical Surveillance Countermeasures Program.
25. DOE 5637.1, CLASSIFIED COMPUTER SECURITY PROGRAM, of 1-29-88, which establishes Departmental requirements for ensuring security of classified information.
26. DOE 5650.2A, CLASSIFICATION OF INFORMATION, of 5-8-85, which specifies responsibilities, authorities, policies, and procedures for the management of the Departmental classification system.
27. DOE 6430.1, GENERAL DESIGN CRITERIA, of 12-12-83, which provides design criteria for use in the acquisition of the Department's facilities.

28. DOE EV 061945, Department of Energy Explosives Safety Manual, which provides information and guidance related to the safe use and storage of explosives.
29. Executive Order 12356, National Security Information, of 4-2-82, which provides requirements concerning classification of information.
30. Federal Specification W-A-450-8, "Interim Federal Specification, Alarm Systems," which provides specifications for interior alarm systems.
31. Federal Specification AA-D-6008, which provides specifications for vaults.
32. "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.
33. National Institute of Justice Standard 0101.02, Ballistic Resistance of Police Body Armor, 2-28-84, which identifies levels of protection for personnel protective armor.
34. National Institute of Justice Report 100-83, which identifies relative incapacitation indices.
35. 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.
36. Title 10 CFR Part 100, Reactor Site Criteria, which guides the evaluation of the suitability of proposed sites for power and test reactors.
37. Title 10 CFR Part 710, Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Significant Quantities of Special Nuclear Materials, of 9-30-77, which establishes policies on personnel clearances.
38. 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.
39. 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.
40. 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.

41. Title 14 CFR Part 108, Airplane Operator Security, which provides requirements for the carriage of weapons and escorted persons while aboard an airplane.
42. 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.
43. Underwriter Laboratories Standard 752, which specifies levels of bullet penetration resistance.
44. Underwriter Laboratories Standard 768, which specifies standards for locks.

DEFINITIONS

1. ACCEPTED RISK. The level of risk that is acceptable to all parties in reference to vulnerabilities on the defined deficiencies on security concerns.
2. ALARM ZONE. An alarm zone is a predesigned segment of the perimeter barrier and isolation zone or a specified area which is protected by one or more intrusion detection aids.
3. ASSESSMENT. An estimation on appraisal, evaluation on analysis.
4. BADGE. (See Identification Badge)
5. CANDLE (OR CANDELA). An international unit of luminous intensity. One candle is equal to the luminous intensity of 5 square millimeters of platinum at its solidification point (1773 C). See also foot-candle.
6. CLASS A FACILITY. Designates a facility which is:
 - a. Judged by Heads of Fields Elements to be engaged in administrative activities considered to be essential to the direction and continuity of the overall program;
 - 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.

7. 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.)
8. CLASS C FACILITY designates a facility which is a:
 - a. Federal Records Center holding classified security interests of the Department;
 - b. A Departmental Administrative Office, 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; or
 - e. Facility in possession of Category III quantities of SNM.
9. 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.
10. 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.

11. CLASSIFIED MATTER. Classified information, documents, parts, components, or other material.
12. 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.
13. COMPETENCY. The ability to perform a task, including whatever knowledge, skills, and attitudes are needed.
14. CONCEALMENT. Protection from hostile observation.
15. CONFIDENTIAL. A classification level which is applied to classified matter of which the unauthorized disclosure could be expected to cause damage to the national security.
16. CONTAIN. To hold an adversary within a defined area or facility for the purpose of preventing the escape of the adversary.
17. CONSTRAINTS. A boundary, limit, or parameter to which the inspection area will be confined.
18. CONTRACTOR. As used in this Order series, the term "contractor" includes subcontractors, consultants, recipients of financial assistance agreements, and another Federal agency in the case of interagency acquisition per DOE 4300.2A.
19. COVER. Protection from hostile fire.
20. COURIER. An authorized person charged with the armed protection of designated matter in transit. 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 arrest without warrant. (These do not include the courier duties of the Federal couriers in the transportation safeguards division.)

21. CRAWLING. Entering and leaving the zone of detection by lying prone to the ground, perpendicular to the zone of detection, moving at an approximate velocity of 0.1 meter per second while maintaining a low profile.
22. CREDENTIAL. A document which identifies and indicates the intended bearer has the authority to perform specific functions (e.g., authority to carry firearms, authority to arrest).
23. CREDENTIAL INSERT. The blank (unused) credential form which is used to prepare the identification badge.
24. CRITERIA. Gauges/measures used to test or compare a real system against the standard or model, such as door thickness, type of lock, or door material.
25. CRYPTO. A designation or marking applied to classified and unclassified telecommunications keying material indicating that it requires special accounting and safeguarding.
26. CUSTODIAN. Any person having assigned responsibility for the control and accountability of classified matter.
27. DANGER AREA. An area which poses increased vulnerability to personnel due to lack of cover and/or concealment, such as roads, parking lots, open areas.
28. DEADLY FORCE. That force which a reasonable person would consider likely to cause death or serious bodily harm.
29. DEFENSE IN DEPTH. Physical protection systems in sufficient strength to constitute more than a single layer of security for a target such as concentric rings of security.
30. DEPARTMENTAL-APPROVED EQUIPMENT. Equipment such as alarms, assessment, monitoring, and detection used in conjunction with all other elements of a site-specific safeguards and security system, as described in a site-specific safeguards and security plan or MSSA that has been approved by the responsible Departmental Element.
31. DEPARTMENTAL PROPERTY. All land, buildings, and structures (real property) and portable equipment, records, and supplies (personal property) which are owned, rented, or leased by the U.S. Government from commercial sources and subject to the administrative custody or jurisdiction of the Department.

32. DETECTION--RECOGNITION--IDENTIFICATION. Detection is the positive assessment that a specific object is the cause of an alarm. Recognition is the positive assessment that the detected object is human, animal, or something else. Identification is the positive assessment of the recognized object as a specific human, animal, or something else.
33. DETECTION ZONE. The volume of space under surveillance of an intrusion detection aid that will cause an alarm when the space is penetrated.
34. 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.
35. ENTRY-LEVEL. The condition that exists when a person is first assigned the duties and responsibilities to perform a job or task.
36. EXCEPTION. An approved alternate means of providing adequate protection. There are two 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 are developed by the Heads of Field Elements and submitted in writing to DP-34 for review and concurrence prior to implementation. Written records of such exceptions are included in the appropriate site-specific safeguards and security plan(s) and/or Master Safeguards and Security Agreement.
 - 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 are developed and approved by the Heads of Field Elements. Written records of such exceptions are included in the appropriate site-specific safeguards and security plan(s) and/or Master Safeguards and Security Agreement.
37. ESCORT. A duty performed by a Department or departmental contractor or common carrier employee specifically responsible for the delivery of a security shipment. Escorts may include protective personnel, truck drivers, and other attendants furnished by the department, departmental

contractors, or common carriers to accompany another person, vehicles, items, or product.

38. EXCLUSION AREA. A security area for the protection of classified matter where mere access to the area would result in access to classified matter.
39. 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.
40. FIELD ELEMENT. Any Departmental organizational component located outside the Washington, D.C., metropolitan area.
41. FOOT-CANDLE (OR CANDELA). A unit of illumination equal to the illumination on the inside spherical surface that is everywhere 1 foot from a uniform point-source of light of 1 candle intensity. See also candle.
42. 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.
43. GUARD. An unarmed Departmental contractor individual who is employed for, and charged with, the protection of classified matter or Government property, excluding SNM (see Security Inspector).
44. HEADQUARTERS STAFF. Heads of Headquarters Elements and employees under their respective jurisdictions.
45. HEAD OF FIELD ELEMENT. The manager of a field element.
46. IDENTIFICATION BADGE. A distinctive badge which provides an individual's name, photograph, and clearance level that may include other information which identifies the bearer. Normally the badge is laminated or otherwise encased to provide a level of tamper resistance.
47. 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.

48. INSTRUCTOR. Any person assigned the task of instructing in a formal training program, regardless of whether that person is a member of the training department staff.
49. ISOLATION ZONE. An area surrounding a facility which has been cleared of any objects which could conceal vehicles or individuals and which affords unobstructed observation, or other means of detection, of entry into the area.
50. 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).
51. JUMPING. Leaping from a height above the zone of detection to a point at ground level across the zone of detection.
52. 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.
53. MASK(ING). The interposition of friendly personnel in the line of fire between other friendly personnel and the adversary.
54. MATERIAL. Any raw, in-process, or manufactured commodity, equipment, component, accessory, part, assembly, or product of any kind.
55. MATERIAL ACCESS AREA. An area containing Category I quantity of SNM specifically defined by physical barriers, located within a protected area, and subject to specific access controls.
56. 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. 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.
57. MATTER. Documents, information, or material.
58. MSSA. Master Safeguards and Security Agreement. An agreement between Headquarters and the field element that defines protection levels and strategies for a facility or security interest.

59. 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.
60. NATIONAL LABORATORY. One of the Department's nine multiprogram laboratories.
61. 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.
62. NEUTRALIZE. To counteract the effectiveness of an adversary force.
63. OPSEC. Operation Security.
64. OUTLAY PROGRAM MANAGERS. Headquarters officials who have lead line responsibility for the execution of authorized programs with appropriated funds.
65. PASS. A temporary authorization to enter an access controlled facility or security area.
66. PERSONAL PROPERTY. Movable items not permanently affixed to, and a part of, the real estate. Generally items remain personal property if they can be removed without serious injury either to the real estate or to the items themselves.
67. PROTECTION FORCE OFFICER. A uniformed Departmental contractor who is employed for, and charged with, the protection of classified matter, DOE property, or other Government property and who is authorized to bear arms in accordance with DOE regulations or local and state authority.
68. 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 contractor, 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.
69. PROGRAM SECRETARIAL OFFICERS. Officer of the Secretary, Secretarial Officers, and DOE Staff Officers.
70. PROPERTY PROTECTION AREA. An area set aside for the protection of property, as required by this Order.
71. PROTECTED AREA. An area encompassed by physical barriers, such as walls or fences, to which access is controlled, and that contains Category II SNM or surrounds a material access area or a vital area, and which meets the standards of this Order.

72. 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.
73. RADIO CIRCUIT DISCIPLINE. Minimizing transmission time by limiting the number and length of transmission and communications to only mission essential items.
74. RANDOM PATROL. A patrol conducted in a manner such that the location of the patrol at any specific time cannot be predicted.
75. REAL PROPERTY. 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 such as buildings, fences, and bridges that are erected 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.
76. REFERENCES. Any approved document to which a rater or an inspected facility's personnel may refer in determining the standards against which a security system is being measured.
77. RELATIVE INCAPACITATION INDEX. An index of the performance of commercially available ammunition and weapons as it concerns the effectiveness of the cartridge to incapacitate.
78. REMOTE INTERROGATION POINTS. Locations for receiving information, such as printouts transmitted by automatic data processing centers.
79. 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. It does not include data declassified or removed from the Restricted Data category, pursuant to section 142 of the Atomic Energy Act.
80. RESTRICTED MATERIAL. Any raw, in process, or manufactured commodity, equipment, component, accessory, part, assembly, or product concerning design, manufacture, or utilization of atomic weapons, protection of special nuclear material, or use of special nuclear material in the production of energy.
81. ROLLING. Entering and leaving the zone of detection prone to the ground, parallel to the zone of detection, and rotating one's body about its long axis at an approximate velocity of 0.1 meter per second while maintaining a low profile.

82. RUNNING. Entering and leaving the zone of detection at an approximate velocity of 5 meters per second.
83. 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.
84. 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.
85. SCRAP. The economically recoverable by-products 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.
86. SECOM. The high frequency radio communications network operated by the Albuquerque Operations Office in support of transportation safeguards.
87. SECRET. The classification level applied to classified matter of which the unauthorized disclosure reasonably could be expected to cause serious damage to the national security.
88. SECURE COMMUNICATIONS CENTER. A security area devoted in whole or in part to the encryption and decryption of sensitive and/or classified information.

89. 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.
90. SECURITY AREA. A physically defined space containing a Departmental security interest and subject to physical protection and access controls.
91. SECURITY CONTAINER.
- a. Security Cabinet. A security cabinet 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. Safe. 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. Vault. A burglar-resistant, windowless enclosure that meets the definition of an SNM vault as given in this Order. Additionally, vaults shall include an intrusion alarm system activated by an opening of the door.
 - d. Vault-type Room. A room having a combination locked door protected by an intrusion alarm system that is 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 (a), (b), and (c) shall meet Underwriter Laboratories Standard No. 768, Group 1-R or other standards which are approved by the field element and provide equivalent protection.
92. SECURITY DISCIPLINE (COMMUNICATIONS SECURITY). Procedures which assure that no classified information or information which could be harmful to the security force or its mission accomplishment (e.g., friendly positions, intentions) is transmitted in clear text over unsecure communications channels.
93. SECURITY FACILITY. Any facility which has been approved by the Department for generating, receiving, using, processing, storing, reproducing, transmitting, destroying classified matter or handling or storing SNM.

94. 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.
95. 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.
96. SECURITY SHIPMENT. A shipment between security areas, DOE facilities, or non-DOE facilities consisting of classified matter or special nuclear material.
97. SEGMENT. A portion of the isolation zone that is alarmed and monitored such that the portion of the isolation zone that is in alarm can be identified.
98. SELF-CHECKING. A feature to ensure secure operation of an alarm system; the system may periodically monitor the sensor transducer and signal processing circuits. Many systems such as vibration, strain, pressure require self-excitation of the sensor transducer, while others such as microwave, infrared, monitor the signal level at the receiving transducer.
99. SENSITIVE COMPARTMENTED INFORMATION. All classified information and materials bearing intelligence community special access controls formally limiting access and dissemination, does not include Restricted Data, as defined in the Atomic Energy Act of 1954, as amended.
100. 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.
101. SENSITIVE MATERIAL. Any raw, in process, or manufactured commodity, equipment, component, accessory part, assembly, or product concerning all classified information and materials bearing intelligence community special access controls formally limiting access and dissemination.
102. SHIELD. A metal (or other material), police-type badge imprinted with the name of the issuing authority, and the serial number of the badge, which provides additional identification of the bearer.
103. SITE SAFEGUARDS AND SECURITY PLAN. A 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.

104. SOURCE MATERIAL. Pursuant to the provisions of section 61 of the Atomic Energy Act of 1954, as amended, 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.
105. 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.
106. SPECIAL NUCLEAR MATERIAL FACILITY. An educational institution, plant, laboratory, office, or building which contains SNM and utilized by the Department, its contractors, subcontractors, or consultants.
107. 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.
108. 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 meets the Class 5 standards set forth in Federal Specification AA-D-6008 of the Federal Specifications and Standards, cited in Title 41 CFR Part 101.
109. STANDARD. For the purposes of these guides, a standard shall be considered as a model established by law, DOE regulation, policy, custom, or general agreement against which a security system can be measured. An example might be that a vault door containing special nuclear material should have a certain delay time against a defined threat.
110. STANDARD WORK CLOTHING. For evaluating closed-circuit television motion detectors, standard work clothing is the equivalent of washed denim jeans and jacket. Such clothing shall be a measure of intruder-to-background contrast.

111. TAMPER-INDICATING. A feature to detect tampering with or unauthorized manipulation of safeguards equipment components. Includes line supervisory circuitry on data transmission lines and switches used to sense the removal of equipment cover plates.
112. TEMPEST. An unclassified term for studies of compromising emanations from electronic or electromechanical equipment processing classified information.
113. TECHNICAL SURVEILLANCE COUNTERMEASURES (TSCM). All measures taken to prevent, detect and neutralize devices used to clandestinely monitor classified activities, for example, wiretap and eavesdrop devices. A TSCM Survey is a detailed examination by specifically trained technicians using sophisticated equipment to locate clandestine technical surveillance devices or other means by which classified activity could be monitored.
114. 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.
115. 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, required to carry out the total responsibility for the safe, secure, domestic transportation of all Departmental-owned or controlled nuclear explosives, Category I or II quantities of SNM (excluding naval reactor core shipments), and other cargos deemed appropriate and agreed to by the Manager, Albuquerque Operations Office, and respective Heads of Departmental Elements.
116. 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.
117. VITAL AREA. A security area located within a protected area for the protection of vital equipment.
118. VITAL EQUIPMENT. Equipment, systems, or components whose failure or destruction would cause unacceptable interruption to a national security program or an unacceptable impact to the health and safety of the public.
119. WALKING. Entering and leaving the zone of detection with a normal stride.

120. 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 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.
121. WEAPON DATA. Classified information, including Restricted Data or Formerly Restricted Data, concerning the design, manufacture, or use, including theory, development, storage, characteristics, performance, and effects, of atomic weapons or components thereof, and information incorporated in or relating to nuclear explosive devices.
122. ZONE (ISOLATION ZONE). The entire perimeter adjacent to the protected area.
123. ZONE OF OBSERVATION--CLOSED-CIRCUIT TELEVISION. The zones of observation for perimeter intrusion alarm assessment by closed-circuit television are those parts of the isolation zone and exterior areas of the protected area extending from the nearest points on the ground viewable by the closed-circuit television camera to the similar point on the ground viewable by an adjacent closed-circuit television camera that is pointed in the same direction or azimuth. Each zone includes the mounting and cable runs of the adjacent camera.

