U.S. Department of Energy

Washington, D.C.

ORDER

DOE 5632.5

2-3-88

SUBJECT: PHYSICAL PROTECTION OF CLASSIFIED MATTER

1. PURPOSE. To establish the Department of Energy (DOE) policy and objectives for the physical protection of classified matter and to establish baseline physical protection requirements and standards for those interests.

2. SCOPE. The provisions of this Order apply to all Departmental Elements, contractors, and subcontractors performing work for the Department as provided by law and/or contract and as implemented by the appropriate contracting officer.

3. POLICY. Classified matter under the jurisdiction of the DOE shall be protected from theft, destruction, loss, or compromise.

4. APPLICABILITY. This Order applies to all classified matter which is in the possession of Departmental Elements or Departmental contractors, but specifically excludes electronic transmissions, which are covered in DOE 5300.1, TELECOMMUNICATIONS. In addition, requirements for control of classified information contained in DOE 5635.1A, CONTROL OF CLASSIFIED DOCUMENTS AND INFORMATION, and DOE 5637.1, CLASSIFIED COMPUTER SECURITY PROGRAM, also apply. NATO classified documents and information shall also be protected under the basic requirements prescribed to in this Order and in accordance with the United States Security Authority Instruction (USSAN 1-69), United States Implementation of NATO Security Procedures. (USSAN 1-69 is available through the U.S. DOE NATO Subregistry.)

5. REFERENCE. DOE 5632.1A, PROTECTION PROGRAM OPERATIONS, of 2-9-88, which establishes policy, responsibilities, and authorities for the physical protection of security interests and contains applicable references and definitions.

6. BASELINE REQUIREMENTS.

   a. Information and guidance regarding implementation of an effective protection program based on these requirements are contained in the Protection Program Operations section of the DOE Safeguards and Security Standards and Criteria. That guidance shall be implemented and documented in accordance with DOE 5632.1A.

   b. Specific hostile actions to be protected against include theft, destruction, loss, or compromise of classified matter.

DISTRIBUTION:
All Departmental Elements

INITIATED BY:
Office of Safeguards and Security

c. A facility shall not receive, use, process, or store classified matter until a facility approval has been granted, based upon a review and acceptance of the facility security plan and/or an on-site survey as required by DOE 5634.1A, SECURITY SURVEYS, NUCLEAR MATERIAL SURVEYS, AND FACILITY APPROVAL.

d. Classification is one factor used in determining the minimum degree of protection required for classified matter. The strategic importance of the matter to national security and other factors such as health and safety considerations shall also be considered in determining the specific protection level provided for specific interests.

e. Requirements for the protection of special nuclear material (SNM) are included in DOE 5632.2A, PHYSICAL PROTECTION OF SPECIAL NUCLEAR MATERIAL AND VITAL EQUIPMENT, and DOE 5633.3, CONTROL AND ACCOUNTABILITY OF NUCLEAR MATERIALS. When SNM is classified because of its configuration or content, or is part of a classified item, it shall receive, as a minimun, the physical protection required by DOE 5632.1A and DOE 5633.3, for the category of SNM involved, or that required by this Order for the assigned classification, whichever is greater.

f. Protect as Restricted Data (PARD) documents shall be protected in accordance with the requirements for the highest classification level involved.

g. Exceptions to specific requirements of this Order may be proposed and processed, consistent with the procedures defined in DOE 5632.1A. Approved exceptions shall be documented and included in the appropriate site safeguards and security plans and/or Master Safeguards and Security Agreements (MSSAs).

h. Classified matter shall be protected appropriately under all conditions. Specific requirements for use, storage, and transfer of classified matter are contained on pages 3 through 15, paragraphs 7, 8, and 9.

i. Controls shall be established to detect and deter unauthorized access to security areas or removal of security interests. Specific requirements for limited areas, exclusion areas, secure communications centers, automated data processing centers, and remote interrogation points processing classified data are contained on page 15, paragraph 10. DOE 6430.1, GENERAL DESIGN CRITERIA, contains further guidelines for design of security areas.

j. Access to security areas or classified matter shall be limited to persons who possess appropriate access authorization or certification and who require such access in the performance of their official duties.

k. A personnel identification system meeting the requirements of DOE 5632.9, ISSUANCE, CONTROL, AND USE OF BADGES, PASSES, AND CREDENTIALS, shall be used.

1. When electronic alarm systems are used to protect classified matter, they shall be designed to meet site-specific protection needs, and, as a minimum, meet the requirements on page 19, paragraph 11.

7. PHYSICAL PROTECTION OF CLASSIFIED MATTER IN USE.

a. Classified matter shall be located within limited or exclusion areas unless those using the matter outside of such areas can protect it against unauthorized access and provide a degree of protection comparable to the requirements of this Order.

b. Classified matter shall not be removed from a limited or exclusion area without appropriate authorization, consistent with the provisions of this Order.

c. Classified matter in use shall be constantly attended by, or under the control of, appropriately cleared personnel responsible for its protection.

d. Persons attending or controlling classified matter shall take appropriate measures to prevent those not having the appropriate clearance and a need-to-know from having access to the matter.

e. Where required by DOE 5635.1A on a site-specific basis, an accountability system shall be maintained to account for and determine when classified matter is lost or unaccounted for. Any inability to account for or any loss of classified matter shall be reported in accordance with DOE 5631.5, VIOLATIONS OF LAWS, LOSSES, AND INCIDENTS OF SECURITY CONCERNS.

f. Classified material and equipment shall bear classification and other necessary extra markings (other than classification) either by stamping, tags, labels, or other suitable means.

g. Automatic data processing (ADP) systems which process, store, transfer, or provide access to classified information may require additional safeguarding as set forth in DOE 5637.1.

8. PROTECTION OF CLASSIFIED MATTER IN STORAGE.

a. Security containers required for the storage of classified matter shall, as a minimum, conform to the following specifications:

(1) A security cabinet is a metal container approved by the General Services Administration for the storage of classified matter.

(2) 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.

(3) A vault is a burglar-resistant, windowless enclosure that meets the definition of a vault. Additionally, such vaults shall include an intrusion alarm system activated by an opening of the door.

(4) 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.

(5) Built-in combination locks on security containers specified in subparagraphs 8a(1), (2), and (3) shall meet Underwriter Laboratories Standard No. 768, Group 1-R, or other standards which are approved by the field element and provide equivalent protection.

b. Requirements for storage are as follows:

(1) Top Secret matter shall be:

(a) In the custody of a Top Secret Control Officer and under continuous armed protective force control; or

(b) Stored in locked, approved security containers:

1 Within a guarded limited or exclusion area under either central station alarm protection; or protective force patrol with inspection of each container at intervals not to exceed 4 hours; or

2 If not located within a limited or exclusion area, under central station alarm protection and protective force patrol at intervals not to exceed 2 hours.

(2) Secret matter shall be stored in a manner authorized for Top Secret matter or at least as secure as one of the following:

(a) Documents located within a limited or exclusion area or other area under protective force control during nonworking periods, shall be:

1 In a locked, approved security container or a steel filing cabinet equipped with a built-in, changeable combination lock; under alarm protection or in an area with protective

force patrols at intervals at least once during each 24 hours of a nonworking period exceeding 1 day; or

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

(b) Documents not located within a limited or exclusion area must be in a locked, approved security container under central alarm station protection or subject to protective force patrols on an 8-hour basis.

(c) Materials, components, and equipment where size, weight, or construction offers substantial resistance to unauthorized removal or surreptitious access to contents shall be:

1 In a locked building of substantial construction or in a locked room within such building. The room or building must be under alarm protection or subject to random guard patrols on an 8-hour basis.

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 under alarm protection, or subject to protective force patrol and inspection at intervals not to exceed 4 hours.

3 In open storage within a single limited or exclusion area, when the classified matter is concealed from unauthorized persons and the storage area is under alarm protection, or subject to protective force patrol and inspection at intervals not to exceed 2 hours.

(d) Materials, components, and equipment which are susceptible to unauthorized removal or surreptitious access shall be protected in the manner set forth in subparagraph 8b(2)(a), (b), or (c), except that protective force patrol, when required, shall occur at intervals not to exceed 2 hours.

(3) 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 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 at intervals not to exceed 8 hours during nonworking periods, as prescribed in this Order.

(b) With respect to materials, components, and equipment:

1 In a security 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 steel filing cabinet equipped with a built-in combination lock or lock bar combination padlock.

(4) 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 5300.3B, TELECOMMUNICATIONS: COMMUNICATIONS SECURITY.

(5) 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 the Office of Safeguards and Security (DP-34) for coordination.

(6) Complete nuclear weapon configurations and nuclear test devices, nuclear explosive like assemblies (NELAs) without nuclear material shall be protected consistent with the highest level and category of classified information they contain.

c. Protective Forces.

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

(2) 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 reported as required by DOE 5631.5.

d. Protective alarms will be responded to by protective force, private security firms, or local law enforcement personnel, as documented in approved security plans.

e. Alternate Storage Locations.

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

(2) Federal Records Centers may be used for the storage of classified information in compliance with DOE 5635.1A.

f. Classified matter retained after completion of contract work agreement shall be safeguarded in accordance with the provisions of this Order. A certificate of possession shall be executed as required by DOE 5635.1A.

9. PROTECTION OF CLASSIFIED MATTER IN TRANSIT.

a. Security shipment of classified matter, including bulk document shipments, are subject to the following conditions:

(1) Contents shall be securely packaged, including double wrapping, where practicable, and shall meet applicable regulations (including Department of Transportation) 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) Approved classified shipping addresses, as specified in the master facility register maintained by the Office of Safeguards and Security, shall be used to assure proper handling upon delivery of a security shipment to the consignee.

(4) Any losses of classified matter, possible violations, or any other unlawful activity during transit must be reported immediately to DP-34.

(5) Contents shall be checked against shipping papers within a time frame specified in approved security plans. Any unresolved discrepancy shall be reported, as required by DOE 5631.5.

(6) The classification level and category 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.

(7) 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.

(8) Combination padlocks shall be used whenever practicable on closed vehicles in addition to seals.

(9) Receipts, listings, and other papers revealing classified information shall be appropriately marked.

(10) Matter in the custody of escorts shall be under their control until delivered or placed in approved storage.

(11) 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.

(12) 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 time and information to enable proper handling at destination.

(13) 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.

(14) Unescorted carload shipments via rail shall be made under arrangements with carriers to furnish a report on request, 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.

(15) 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.

b. Protective services for Departmental security shipments are available as follows:

(1) Appropriately authorized and cleared Departmental or Departmental contractor personnel, designated by name or title and upon written authority of the responsible manager, may handcarry, transport, or escort Secret or Confidential matter.

(2) 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. 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. Use of these options shall be based upon protection meeting the minimum security requirements outlined in subparagraphs (a) and (b) below.

(a) Spot checks shall be conducted as specified in approved security plans to verify compliance with the minimum security requirements.

(b) 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, it shall be locked while in transit.

c. Approved means of shipment.

(1) Security shipments moving entirely within the United States are protected as follows:

(a) Top Secret matter, excluding Top Secret communications security matters, shall be transported in the custody of Department-approved couriers.

(b) Top Secret communications security matter may be transported in the custody of two escorts, either Departmental 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 Departmental or Departmental contractor personnel having "Q" access authorization;

4 Aircraft under Departmental contract with pilots who hold "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 report identifying the car location; or

c Air carriers providing 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 the 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. certified (return receipt requested) or express mail;

3 Airlines under Departmental contract, or U.S. Government aircraft, with pilots holding "L" access authorization or Department of Defense 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 are protected as follows:

(a) Top Secret matter, 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 facilities, provided the approval of DP-34 is obtained and information does not pass out of U.S. citizen control and 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.

d. Courier and escort duties, not including the courier duties of the DOE couriers in the Albuquerque Operations Transportation Safeguards Division, are as follows:

(1) Courier duties may be performed by a qualified 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) A sufficient number of couriers or other escorts required to perform the above functions shall be assigned to a shipment, including relief personnel.

(4) 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.

(5) Couriers and escorts shall possess identification cards. They shall be issued by the Heads of the Field Element (or DP-34 for Headquarters) or the responsible contractor security office, as

applicable. Couriers and escorts shall carry identification cards 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. Any courier authorized to carry a firearm aboard a commercial or public-owned aircraft shall comply with the rules and regulations set forth in Title 14 CFR Part 108.

(6) Couriers and 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 couriers and escorts while assigned to a security shipment operation is prohibited.

(7) Specific instructions and operating procedures shall be prepared in detail and issued to escorts prior to each shipment.

(8) Couriers shall be "Q" cleared. 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. An "L" or "S" access authorization is sufficient if there is not access to Restricted Data. 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.

(9) 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, 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 and 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 of classified matter via commercial or military aircraft, provide continuous observation of plane and cargo during ground stops and of cargo during loading and unloading operations.

10. SECURITY AREAS AND ACCESS CONTROL REQUIREMENTS.

a. Security areas shall be established when the nature, size, revealing characteristics, sensitivity, or importance of the classified matter or associated security interests is such that access to them cannot be effectively controlled by other internal measures. Offices of consultants or other individuals, small laboratories, or other facilities with narrow scope and low volume of work involving classified matter normally do not require establishment of security areas; however, adequate security measures must be in place to preclude unauthorized access.

(1) A Limited Area is a security area which is established for protection of classified matter where security officers, security police officers, or other internal controls can prevent access to classified matter by unauthorized persons.

(2) Protected Areas are security areas which are established for protection of special nuclear material or vital equipment. Protected areas meet the requirements for a Limited Area as long as measures are taken to prevent unauthorized visual or aural access to classified information.

(3) An Exclusion Area is a security area which is established for protection of classified matter where mere presence in the area would normally result in access to classified information.

(4) Security areas are also established to protect ADP processing centers and remote interrogation points, secure communications centers, sensitive compartmented information facilities, and facility alarm system central stations.

b. Limited Area requirements:

(1) Clearly defined physical barriers such as fences, walls, and doors shall be utilized to define the perimeter of the security

area and control, impede, or deny access, and shall effectively direct the flow of personnel and vehicles through designated portals, and permit effective inspections. Permanent barriers shall be used to enclose security areas except during construction or transient activities, when temporary barriers may be erected.

(2) Personnel and vehicle access controls are as follows:

(a) Verification of the identity of persons authorized access to a Limited Area shall be accomplished at the area entrance.

(b) A visitor log shall be maintained to reflect the name, signature, organization, and citizenship of each uncleared visitor to a limited area, persons visited, escort names and signatures, purpose of visit, and time in and out.

(c) A visitor without appropriate access authorization or certification shall be escorted at all times by an appropriately cleared and knowledgeable person.

(3) All vehicles, all personnel (cleared and uncleared), and all handcarried items entering Limited Areas shall be subject to inspection to deter the unauthorized introduction of explosives, weapons, cameras, electronic recording or transmitting equipment, or other prohibited articles. Inspections shall be conducted on a random basis at frequencies as specified in the applicable site safeguards and security plan and/or Master Safeguards and Security Agreement.

(4) All vehicles, all personnel (cleared and uncleared), and all handcarried items exiting Limited Areas shall be subject to inspection to deter the unauthorized removal of classified matter or Government property. Inspections shall be conducted on a random basis at frequencies as specified in the applicable site safeguards and security plan and/or Master Safeguards and Security Agreement.

(5) Signs prohibiting trespass shall be posted around the perimeter of the security area and at each entrance. 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.

(6) A means shall be provided to detect unauthorized intrusion by use of alarm systems, random patrols, or visual surveillance. Procedures to meet this requirement shall be documented in approved site safeguards and security plans and/or Master Safeguards and Security Agreements.

(7) Protective illumination shall be provided to permit or assist in detection and assessment of adversaries, reveal unauthorized persons, and, at pedestrian and vehicular entrances, permit examination of credentials and vehicles.

(8) The protection program shall include suitable means to assess alarms and/or activities of adversaries.

(9) Measures shall be in place to prevent unauthorized visual or aural access to classified matter as required by DOE 5636.3A, TECHNICAL SURVEILLANCE COUNTERMEASURES PROGRAM.

(10) All security-related subsystems and components shall have a regularly applied test and maintenance program to assure an effective operable system. Compensatory measures shall be implemented when security-related subsystems or components are not in service, as defined in an approved security plan.

c. Exclusion area requirements are as follows:

(1) 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.

(2) When access to an exclusion area is required by persons without appropriate access authorization or need-to-know, measures shall be taken to prevent access to or compromise of classified information.

(3) An exclusion area must meet all the requirements listed in paragraph 10b for a limited area; except that when the exclusion area is located within a larger limited area, additional trespass signs are not required, additional inspections/searches need not be performed, and an unattended access control system may be used.

d. ADP systems which process, store, transfer, or provide access to classified information shall be protected according to requirements in DOE 5637.1.

e. Requirements for secure communications centers are as follows:

(1) Communications centers handling classified messages shall be established as limited areas and meet the requirements defined

in paragraph 10b or be within an established security area located within larger limited areas.

(2) When contained within a larger limited area, a secure communications center shall be established as a security interest and have separate access controls and barriers to restrict admittance to persons who require access in the performance of official duties.

(3) 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.

f. Requirements for sensitive compartmented information facilities are as follows:

(1) Sensitive compartmented information facilities shall be established as limited areas and meet the requirements defined in paragraph 10b or be located within a larger limited area.

(2) When contained within a larger limited area, a sensitive compartmented information facility shall be established as a security interest and must have separate access controls and barriers to restrict admittance to persons who require access in the performance of official duties.

(3) 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 sensitive compartmented information facilities. A list of persons authorized such access shall be posted at the entrance to the facility and a record of all visitors shall be maintained.

g. Requirements for central alarm stations are as follows:

(1) Facility central alarm stations shall located within, or established as, security areas and be constantly attended by assigned personnel.

(2) Central alarm stations shall have 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.

11. INTRUSION DETECTION EQUIPMENT.

a. Devices and equipment for interior intrusion detection systems used to protect classified matter in storage shall meet Federal specification W-A-450-B, "Interim Federal Specifications, Alarm Systems," or be approved by the field element.

b. Exterior sensors that serve as the primary means of detection at a security area perimeter shall be designed to provide assurance that a person crossing the perimeter will be detected whether walking, running, jumping, crawling, rolling, or climbing, at any point in the detection zone.

c. Intrusion alarm systems shall be monitored continuously by personnel who can initiate an appropriate response.

d. Response to alarms shall be timely. Site-specific response plans shall be documented in applicable site safeguards and security plans and/or MSSAs.

e. 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 of the recorder and date of recording shall appear in such record. Recording of such alarms by automatic means is permissible if the automatic system records the identity of the operator on duty.

f. Copies of each nonscheduled alarm report shall be furnished to the facility security officer and field element personnel as specified in approved security plans.

g. All security-related detection equipment and components shall have a regularly applied test and maintenance program to assure an effective operable system. The required frequency of routine testing and maintenance activities shall be established and documented in field element approved security plans.

h. Intrusion alarm systems shall have a primary and auxiliary power source. Switch over to the auxiliary power source shall be immediate and automatic in case of failure of the primary power source. An alarm condition shall be indicated at the monitor upon failure of power sources.

i. Alarm lines shall be continuously supervised to detect attempts to short, open, or substitute a bogus signal for the legitimate "no alarm" signal in a surreptitious attempt to bypass the alarm system.

j. Plant protection force personnel responding to intrusion detection alarms used for the protection of classified matter located within exclusion areas shall possess "Q" access authorization when Top Secret or Secret Restricted Data matter or SNM is involved and "L" access authorization, 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.

k. Plant protection 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 police or commercial protective service personnel monitoring, installing, maintaining, or responding to alarms shall be obtained.

l. Personnel testing, maintaining, or servicing alarms shall have clearances consistent with the highest classification levels being protected, and as noted in subparagraphs j and k, above, unless such testing and maintenance is performed as bench services away from the protected location, or is performed under the supervision of an appropriately cleared and knowledgeable custodian of the alarm protected location. Alarms bench tested or maintained by uncleared personnel away from the protected location shall be inspected and tested prior to installation.

BY ORDER OF THE SECRETARY OF ENERGY:

LAWRENCE F. DAVENPORT
Assistant Secretary
Management and Administration