

Approved: 12-23-02

**SUBJECT: PHYSICAL PROTECTION PROGRAM**

---

1. OBJECTIVE. To establish Department of Energy (DOE) management objectives, requirements and responsibilities for the physical protection of safeguards and security (S&S) interests. To provide program requirements for the physical protection of S&S interests. (See DOE M 473.1-1, *Physical Protection Program Manual*, dated 12-23-02.)
2. CANCELLATION. DOE 5632.1C, *Protection and Control of Safeguards and Security Interests*, dated 7-15-94. Cancellation of this Order does not modify or otherwise affect any contractual obligation to comply with the Order. If the cancelled Order is incorporated by reference in a contract, it remains in effect until the contract is modified to delete the reference to the requirements in the cancelled Order.
3. APPLICABILITY.
  - a. DOE Elements. Except for the exclusions in paragraph 3c, this Order applies to all DOE elements listed in Attachment 1, including the National Nuclear Security Administration (NNSA).
  - b. Site/Facility Management Contracts.
    - (1) The Contractor Requirements Document (CRD), Attachment 2, sets forth requirements of this Order that will apply to contractors responsible for the management and operation of Department-owned facilities (hereafter referred to as site/facility management contractors) whose contracts include the CRD.
    - (2) This CRD must be included in all site/facility management contracts that contain the clause at 48 CFR 952.204-2, Security Requirements.
    - (3) This Order does not automatically apply to other than site/facility management contracts. Application of any of the requirements of this Order to other than site/facility management contracts will be communicated separately from this Order. (See paragraphs 5k through 5n.)
    - (4) The officials identified in paragraphs 5k through 5n are responsible for notifying the contracting officers of which contracts are affected. Once notified, contracting officers are responsible for incorporating the CRD

into the affected contracts via the laws, regulations, and DOE directives clause of the affected contracts.

- (5) As the laws, regulations, and DOE directives clause of site/facility management contracts states, regardless of the performer of the work, site/facility management contractors with the CRD incorporated into their contracts are responsible for compliance with the requirements of the CRD. Affected site/facility management contractors are responsible for flowing down the requirements of this CRD to subcontracts at any tier to the extent necessary to ensure compliance with the requirements.

c. Exclusions.

- (1) Facilities and activities regulated by the Nuclear Regulatory Commission and the Office of Civilian Radioactive Waste Management are exempt from this Order.
- (2) Shipments mandated by the Nuclear Waste Policy Act, as amended, and managed by the Office of Civilian Radioactive Waste Management are exempt from this Order.
- (3) Consistent with the responsibilities identified in Executive Order 12344, the Director of the Naval Nuclear Propulsion Program will determine the applicability of this Order for activities and facilities under his/her control.

d. Deviations. Deviations from the protection requirements prescribed by this Order and the associated Manual must be processed in accordance with DOE O 470.1, *Safeguards and Security Program*, dated 9-28-95.

4. REQUIREMENTS. Site physical protection programs must be systematically executed, evaluated, and documented as described by a site safeguards and security plan (SSSP) or security plan in accordance with DOE O 470.1. Develop physical protection programs based on the current "Department of Energy Design Basis Threat Policy for the Department of Energy Programs and Facilities (U)."

- a. Safeguards and Security Interests. DOE assets must be protected from malevolent acts and from events such as disasters and civil disorders through the consideration of: site and regional threats, protection planning, strategies, and protection measures. Special nuclear material (SNM) must be protected at the higher level when roll-up occurs within a single security area unless the facility has conducted a vulnerability assessment that determined the failure or defeat of protection measures would not increase the risk. DOE may impose, within its authority, requirements deemed necessary to protect the safety of employees and the public and to minimize threats to life, SNM, radiological/chemical/biological materials, classified matter, Government property, and/or the environment.

- b. Program Integration. The physical protection program must be integrated with other programs, such as protective force, materials control and accountability, emergency operations, weapons surety, personnel security, foreign visits and assignments, and information security, to achieve total integration of S&S programs.
- c. Physical Protection Program Elements. The physical protection program's integrated elements include all protection program operations, security areas, protective personnel, systems, and subsystems tailored to provide site-specific protection of S&S interests. With the exception of property protection areas, these interests must be protected using a concentric security area approach.
  - (1) Concentric Security Areas. Layers of security requirements, beginning with the least restrictive and moving inward to the most restrictive, must be implemented for protecting DOE S&S interests.
    - (a) The requirements for property protection areas must be configured to protect Government-owned property and equipment against damage, destruction, or theft and must provide a means to control public access. Requirements must be locally developed, implemented, and approved by the cognizant DOE approving authority.
    - (b) DOE security areas designated as limited areas, exclusion areas, protected areas, vital areas, or material access areas are established to protect S&S interests. These areas must be defined by permanent barriers; access to these security areas must be controlled.
  - (2) Intrusion Detection Capability. Intrusion detection systems (IDSs) and/or visual observations by protective force personnel must be used to detect unauthorized entry and/or presence in security areas. (See DOE M 473.1-1.)
    - (a) Ensure that breaches in security areas are detected and alarms annunciated.
    - (b) Ensure that perimeter intrusion detection and assessment systems protecting Category I and II quantities of SNM use multilayered, complementary intrusion detection sensors.
    - (c) Ensure that an effective method is established to assess all IDSs and access control alarms (including tamper and supervisory alarms) to determine the cause of alarms.
  - (3) Alarm Management and Control Systems.

- (a) Intrusion and access control system alarms protecting Category I and II SNM must annunciate simultaneously at a central alarm station (CAS) and a secondary alarm station (SAS).
    - 1 The CAS must be a hardened post, manned 24 hours a day, and located, at a minimum, within a limited area.
    - 2 A SAS must be used as an alternative alarm annunciation point to the CAS and must be maintained at a location manned 24 hours a day such that a response can be initiated in the event the CAS is unable to perform its intended function. The SAS need not be fully redundant to the CAS, but must be capable of providing control to S&S incidents.
  - (b) Tamper and supervisory alarms must be assessed by protective force personnel. Technical/maintenance support personnel must conduct followup assessment of tamper and supervisory alarms.
  - (c) Closed circuit television used for primary assessment must use fixed cameras that provide a clear image for assessment.
  - (d) Video recording of assessment cameras must capture information for alarm assessment.
- (4) Access Controls and Entry/Exit Inspections.
- (a) Access to security areas must be controlled. Access must be based on access authorizations and need to know.
  - (b) A person without an access authorization who is permitted to enter a limited area, exclusion area, protected area, vital area, or material access area must be escorted at all times by a designated individual, trained in escort duties and possessing the required access authorization.
  - (c) Personnel, hand-carried items, deliveries/mail, vehicles, and vehicle contents are subject to random inspections at security area boundaries except for protected areas and material access areas where inspections must be conducted.
- (5) Barriers. Permanent physical barriers must be installed to control, deny, impede, or delay unauthorized access into security areas. Security areas must be delineated by separate and distinct permanent barriers. The

requirement for barriers at property protection areas must be locally implemented and included in security plans.

- (6) Secure Storage. S&S interests requiring secure storage must be placed in vaults, vault-type rooms, vault-type-room complexes, and/or General Services Administration—approved security containers.
- (7) Protective Personnel. Protective personnel include the protective force personnel designated as security officers; security police officers (SPOs); federal officers/special agents; and persons assigned administrative or other security duties. (See DOE O 473.2, *Protective Force Program*, dated 6-30-00, and DOE M 473.2-2, *Protective Force Program Manual*, dated 6-30-00.)
- (8) Communications.
  - (a) Voice communications systems used for security purposes must provide intelligible voice communications in all security areas for all modes of operation and operating conditions. Special response team communication equipment must be equipped with digital encryption. Special response team communications must have channels separate from normal operating channels.
  - (b) Security system transmission lines and data must be protected in a graded manner from tampering and substitution.
- (9) Testing and Maintenance.
  - (a) The effectiveness of physical protection systems and programs must be determined through performance testing as required by the DOE Performance Assurance Program. (See DOE O 470.1.)
  - (b) A program of scheduled testing and maintenance must be implemented to ensure an effective, fully functional security system. (See DOE M 473.1-1.)
- (10) Posting. Post signs, where applicable, with information on the Atomic Weapons and Special Nuclear Materials Rewards Act; prohibited and/or controlled articles; entry and exit inspections of vehicles, packages, and persons; and trespassing under Section 229, Atomic Energy Act of 1954, as amended. Post signs prohibiting trespassing around the perimeter and at each entrance to a security area except when one security area is located within a larger posted security area.
- (11) Badges. A DOE-issued badge must be worn at all times while in security areas, including property protection areas, on DOE-owned or DOE-leased

property. The DOE badge may not be used outside of DOE for other-than-Government purposes.

d. Physical Protection Surveillance Equipment.

- (1) Physical protection surveillance equipment must be used for the purposes described in an SSSP or security plan. Programs and procedures must be developed to prohibit misuse of physical protection surveillance equipment (e.g., video assessment and audio communication/recording equipment). NOTE: Physical protection surveillance equipment, when used in accordance with this requirement, is not considered technical surveillance equipment.
- (2) Signs must be posted to serve notice that physical protection surveillance equipment is operating.

e. Implementation. Implementation plans for any requirement that cannot be implemented within 6 months of the effective date of this Order or within existing resources must be developed by heads of DOE elements and submitted for approval to the respective program offices. Copies of the plans must be forwarded to the Office of Security.

5. RESPONSIBILITIES.

a. Heads of DOE Elements.

- (1) Ensure physical security programs under their cognizance are implemented in conformance with Department security policies.
- (2) Evaluate physical protection programs to ensure effectiveness and compliance with the Department's protection requirements.
- (3) Review procurement requests for new non-site-/non-facility-management contracts, and if appropriate, ensure that the clause at 48 CFR 952.204-2, Security Requirements, and the requirements of the CRD of this directive are included in the contract.

b. Director, Office of Security. Develops, coordinates, promulgates, and clarifies policies, standards, and requirements for the DOE physical protection program. Maintains national-level liaison with other Federal law enforcement, security, and intelligence agencies in support of the physical protection program.

c. Director, Office of Emergency Operations. Coordinates the emergency preparedness program with the S&S protection program for emergencies created by malevolent threats or acts and disasters.

- d. Director, Office of Intelligence. Develops, in conjunction with the director, Office of Security, programs and procedures to protect Foreign Intelligence Information and Sensitive Compartmented Information held within DOE and contractor facilities.
- e. Administrator, National Nuclear Security Administration. In addition to the responsibilities in paragraphs 5a and 5k, the NNSA Administrator ensures the development, coordination, and implementation of this Order and the associated Manual and other DOE directive requirements relating to the physical protection of S&S interests.
- f. Assistant Secretary for Environment, Safety and Health. Assists in the development of physical protection policy issues to ensure environmental, safety, medical, and health considerations are properly integrated.
- g. Director, Office of Independent Oversight and Performance Assurance. Through the director, Office of Safeguards and Security Evaluations, provides independent inspections and evaluations to assess the effectiveness of S&S programs implemented under this Order and the associated Manual.
- h. Assistant Secretary for Environmental Management. In addition to the responsibilities in paragraphs 5a and 5k, the Assistant Secretary for Environmental Management provides the primary point of contact with the transportation industry and with Federal, State, and local agencies in implementing DOE transportation policies and standards for protection of hazardous material, other than nuclear explosives, SNM, or other classified matter.
- i. Director, Office of Science. In addition to the responsibilities in paragraph 5a, the director, Office of Science, designs and establishes procedures for the issuance and use of the DOE Office of Science Badge, in coordination with the director, Office of Security, to ensure DOE S&S interests are adequately protected.
- j. Director, Naval Nuclear Propulsion Program. In accordance with the responsibilities and authorities assigned by Executive Order 12344, as prescribed by Public Law 98-525 (42 U.S.C. 7158), and to ensure consistency throughout the joint Navy/DOE organization of the Naval Nuclear Propulsion Program, implements and oversees all pertinent requirements for activities under the Director's cognizance.
- k. Program Secretarial Officers.

- (1) Ensure facilities under their cognizance have implemented this Order.
- (2) Notify contracting officers of affected site/facility management contracts that must include the CRD of this Order.
- (3) Ensure procurement requests for new non-site-/non-facility-management contracts require inclusion of the clause at 48 CFR 952.204-2, Security Requirements, and this Order's CRD in the resulting contracts, if appropriate.

1. Heads of Field Elements.

- (1) In addition to the responsibilities in paragraph 5a, oversee physical protection programs to ensure DOE S&S interests are protected.
- (2) Ensure the development and maintenance of directives, plans, and procedures for the operation, maintenance, and testing of physical protection programs to protect S&S interests.
- (3) Oversee contractor development, implementation, and management of physical protection programs in conformance with this Order.
- (4) Ensure the physical protection program requirements of this Order, the associated Manual, and other S&S directives are implemented.
- (5) Ensure the provisions established within this Order and the associated Manual are included in contracts.
- (6) Ensure DOE and contractor employees receive appropriate S&S-related training and are made aware of and understand their responsibilities for protecting S&S interests.
- (7) Inspect, test, and evaluate the physical protection programs, projects, and facilities of subordinate activities to ensure effectiveness and compliance with protection requirements.
- (8) Recommend to the director, Office of Security, through the lead program Secretarial offices, for publication in the Federal Register, property to be designated for "No Trespassing" posting under 42 U.S.C. 2278a, and ensure that "No Trespassing" notices are posted.
- (9) Provide physical protection for S&S interests while in transit.
- (10) Review procurement requests for new non-site-/non-facility-management contracts, and if appropriate, ensure that the clause at 48 CFR 952.204-2,



Security Requirements, and the requirements of the CRD of this Order are included in the contract.

m. Contracting Officers.

- (1) After notification by the appropriate program official, incorporate the CRD into affected site/facility management contracts in accordance with the laws, regulations, and DOE directives clause of the contracts.
- (2) Assist originators of procurement requests who want to incorporate the clause at 48 CFR 952.204-2, Security Requirements, and the requirements of the CRD of this Order in new non-site-/non-facility- management contracts, as appropriate.

6. DEFINITIONS. See DOE M 473.1-1.

7. REFERENCES.

- a. DOE M 251.1-1A, *Directives System Manual*, dated 1-30-98.
- b. DOE O 470.1, *Safeguards and Security Program*, dated 9-28-95.
- c. DOE O 471.2A, *Information Security Program*, dated 3-27-97.
- d. DOE M 471.2-1B, *Classified Matter Protection and Control Manual*, dated 1-6-99.
- e. DOE M 471.2-1C, *Classified Matter Protection and Control Manual*, dated 4-17-01.
- f. DOE M 473.1-1, *Physical Protection Program Manual*, dated 12-23-02.
- g. DOE O 473.2, *Protective Force Program*, dated 6-30-00.
- h. DOE M 473.2-2, *Protective Force Program Manual*, dated 6-30-00.
- i. DOE 142 Series, Foreign Visits and Assignments.
- j. *Design Basis Threat for Department of Energy Programs and Facilities (U)*, dated February 1999.
- k. *Technical Surveillance Countermeasures Procedural Manual*, dated October 1994 (U). (This is an Office of Security document for limited distribution. Please call 301-903-3653 to request a copy).

8. CONTACT. Questions concerning this Order should be directed to the program manager, Protection Program Operations, at 301-903-6209.

BY ORDER OF THE SECRETARY OF ENERGY:



KYLE E. McSLARROW  
Deputy Secretary

**DEPARTMENT OF ENERGY ORGANIZATIONS TO WHICH  
DOE O 473.1, *Physical Protection Program*, IS APPLICABLE**

Office of the Secretary  
Office of the Chief Information Officer  
Office of Civilian Radioactive Waste Management  
Office of Congressional and Intergovernmental Affairs  
Office of Counterintelligence  
Departmental Representative to the Defense Nuclear Facilities Safety Board  
Office of Economic Impact and Diversity  
Office of Energy Efficiency and Renewable Energy  
Energy Information Administration  
Office of Environment, Safety and Health  
Office of Environmental Management  
Office of Fossil Energy  
Office of General Counsel  
Office of Hearings and Appeals  
Office of Independent Oversight and Performance Assurance  
Office of the Inspector General  
Office of Intelligence  
Office of Management, Budget and Evaluation and Chief Financial Officer  
National Nuclear Security Administration  
Office of Nuclear Energy, Science and Technology  
Office of Policy and International Affairs  
Office of Public Affairs  
Office of Science  
Secretary of Energy Advisory Board  
Office of Security  
Office of Worker and Community Transition  
Office of Energy Assurance  
Bonneville Power Administration

Southeastern Power Administration  
Southwestern Power Administration  
Western Area Power Administration

## CONTRACTOR REQUIREMENTS DOCUMENT

### DOE O 473.1, *Physical Protection Program*

This Contractor Requirements Document (CRD) addresses physical protection programs and the protection of safeguards and security (S&S) interests. (See requirements contained in DOE M 473.1-1, *Physical Protection Program Manual*.) Physical protection programs must be documented in a site safeguards and security plan (SSSP) or security plan. (See DOE O 470.1, *Safeguards and Security Program*, dated 9-28-95.) Regardless of the performer of the work, the contractor is responsible for compliance with the requirements of this CRD. The contractor is responsible for flowing down the requirements of this CRD to subcontracts at any tier to the extent necessary to ensure the contractor's compliance with the requirements. The contractor will do the following.

1. Identify and protect S&S interests. The S&S interests include but are not limited to classified matter, special nuclear material and other nuclear materials, secure communications centers, sensitive compartmented information facilities, automated data processing centers, facilities storing and transmitting classified information, or vital equipment.
2. Develop physical protection programs based on the current *Department of Energy Design Basis Threat Policy for the Department of Energy Programs and Facilities (U)*, dated February 1999. The physical protection program must consider site and regional threats, malevolent acts, and emergency situations, such as civil disturbances and disasters.
3. The SSSP or security plan must fully describe the implementation of all protection element requirements. (See DOE M 473.1-1.)
  - a. Protection Strategies. Each site must develop and delineate protection strategies for all S&S interests. (See DOE O 470.1.)
  - b. Contingency/Emergency Planning. Ensure that a plan for the physical protection of S&S interests in the event of an emergency, disaster, or civil disturbance is developed, implemented, and performance tested.
4. Develop physical protection measures based on a protection strategy that specifically addresses the S&S interests identified.
  - a. Graded Protection. Provide a graded physical protection program to S&S interests in a cost-effective manner consistent with potential threats.
  - b. SNM Roll-Up. Protect special nuclear material (SNM) at the higher level if a roll-up situation could develop within a single security area unless the facility has conducted a vulnerability assessment that determined the failure or defeat of protection measures will not increase the risk.

- c. Risk Management. Rely on risk management principles as the underlying basis for making security related decisions for an enduring protection program. Accordingly, ensure that asset valuations, threat analyses, and vulnerability assessments are considered in determining risk.
  - d. Outside Agency Protection Support. Describe support provided by outside agencies for DOE S&S incidents in the SSSP or security plan.
5. Provide site-specific S&S protection or tailor the physical protection elements, including the following.
- a. Security Areas. Establish security areas to protect S&S interests.
  - b. Intrusion Detection Capability. Use intrusion detection systems (IDSs) and/or visual observations by protective force personnel to detect unauthorized entry and/or presence in security areas that require protection.
    - (1) Ensure breaches in the security area boundaries for those S&S interests under IDS protection are detected and alarms are annunciated.
    - (2) Ensure perimeter intrusion detection and assessment systems protecting Category I and II quantities of SNM use multilayered, complementary detection sensors.
    - (3) Ensure IDSs protecting Category I and II quantities of SNM and other high-consequence assets are monitored at a central alarm station (CAS).
    - (4) Ensure all IDSs and access control alarms are effectively assessed to determine the cause of alarms.
  - c. Alarm Management and Control Systems.
    - (1) Ensure intrusion and access control system alarms protecting Category I and II SNM annunciate at both a CAS and a secondary alarm station (SAS).
      - (a) Ensure the CAS is a hardened post, manned 24 hours a day, and located, at a minimum, within a limited area.
      - (b) Intrusion detection and assessment system components, sensors, and communication systems must be protected by tamper and supervisory alarms.

- (c) A SAS must be used as an alternative alarm annunciation point to the CAS and must be maintained at a location continuously manned such that a response can be initiated in the event a CAS is unable to perform its intended function. The SAS need not be fully redundant to the CAS.
  - (2) Ensure all tamper and supervisory alarms are assessed by the protective force. Technical/Maintenance support personnel must conduct followup assessment of tamper and supervisory alarms.
  - (3) Ensure closed circuit television used as the primary assessment tool uses fixed cameras and provides a clear image for assessment.
  - (4) Ensure video recorded from assessment cameras capture information necessary for alarm assessment.
- d. Access Controls and Entry/Exit Inspections. Personnel, hand-carried items, deliveries/mail, vehicles, and vehicle contents are subject to random inspections at security area boundaries except for protected areas and material access areas where inspections must be conducted.
  - (1) Ensure access to security areas is controlled. Access must be based on access authorizations and an individual's need to know in order to perform official duties. An approved DOE security badge validates an individual's access authorization but does not constitute a need to know. Need to know determinations must be made before granting individuals access to classified matter.
  - (2) Ensure persons without appropriate access authorizations who are allowed to enter limited areas, exclusion areas, protected areas, vital areas, or material access areas as visitors are escorted at all times by individuals with—
    - (a) knowledge of security procedures for those security areas listed above,
    - (b) appropriate access authorizations, and
    - (c) need to know for the security areas or S&S interests.
- e. Barriers. Install permanent physical barriers to control, deny, impede, or delay unauthorized access into all security areas. Delineate DOE-designated security areas by means of separate and distinct permanent barriers. The requirement for

barriers at property protection areas must be locally implemented and included in security plans.

- f. Secure Storage. S&S interests requiring secure storage must be placed in vaults, vault-type rooms, vault-type-room complexes, and/or General Services Administration—approved security containers.
- g. Protective Personnel. Protective personnel include the protective force personnel designated as security officers; security police officers (SPOs); federal officers/special agents; and persons who have administrative responsibilities or who are assigned other security duties. (See DOE O 472.2, *Protective Force Program*, dated 6-30-00 and DOE M 473.2-2, *Protective Force Program Manual*, dated 6-30-00.)
- h. Communications.
  - (1) Ensure voice communications systems used for security purposes are operable and provide intelligible voice communications in all security areas for all modes of operation.
  - (2) Ensure security system data transmission lines and data are protected in a graded manner from tampering and substitution.
- i. Testing and Maintenance.
  - (1) Performance test physical protection systems and programs to measure effectiveness. The performance assurance program must identify critical subsystems, components, and time intervals between tests.
  - (2) Implement a program of scheduled testing and maintenance to ensure an effective, operable security system.
- j. Posting. Post signs, where applicable, with information on the Atomic Weapons and Special Nuclear Materials Rewards Act; prohibited and controlled articles; entry and exit inspections of vehicles, packages, or persons; and trespassing. Post signs prohibiting trespassing around the perimeter and at each entrance to a security area except when one security area is located within a larger posted security area.
- k. Security Badges. Ensure that a DOE badge is issued to employees and that it is worn at all times while in DOE-owned or leased security areas, including property protection areas. The Office of Science badge is only authorized at Office of Science property protection facilities.



- (1) Ensure the DOE security badge is used to gain access to DOE and contractor operated facilities, S&S interests, and/or security areas, and ensure the Office of Science badge is not used for access to DOE facilities that require the DOE security badge.
- (2) Ensure the DOE security badge is not used outside of DOE for other-than-Government purposes.

6. PHYSICAL PROTECTION SURVEILLANCE EQUIPMENT USE.

- a. Develop programs and procedures to deter misuse of physical protection surveillance equipment (e.g., video assessment equipment). Document in the SSSP or in the security plan that the physical protection surveillance equipment must be used for the stated purposes. NOTE: Physical protection surveillance equipment, when used in accordance with this requirement, is not considered technical surveillance equipment and, therefore, is not subject to the requirements for technical surveillance equipment.
- b. Post signs to serve notice that physical protection surveillance equipment is operating.