

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

ORDER

DOE 5631.1

7-28-80

SUBJECT: SAFEGUARDS AND SECURITY AWARENESS PROGRAM

1. PURPOSE. This Order establishes the policy for and implementation of a systematic safeguards and security awareness program for the Department of Energy (DOE) and its consultants, and for DOE contractors, subcontractors, and their consultants, DOE access permittees, and the Federal Energy Regulatory Commission (FERC), in compliance with the provisions of the Atomic Energy Act of 1954, as amended, and Executive Order 12065, National Security Information. The goal of this program is to instruct and inform personnel and subsequently maintain an appropriate awareness of safeguards and security measures and policies to assure maximum protection of national security interests.
2. SCOPE. The provisions of this Order are applicable to all Departmental elements, including the Federal Energy Regulatory Commission, and to consultants, contractors, subcontractors, and their consultants.
3. POLICY. DOE requires the formulation and maintenance of a structured safeguards and security awareness program in all organizations where employees are granted access authorizations, are engaged in any classified work, require access to special nuclear material, or are engaged in the protection of or control over access to special nuclear material.
  - a. The formulation and implementation of this program is intended to:
    - (1) Involve mandatorily DOE and DOE contractor employees personally in the promotion of an effective safeguards and security awareness program.
    - (2) Assure that employees are knowledgeable of and understand the security requirements applicable to them and their assignments.
    - (3) Alert employees to actual or potential threats to DOE security and other interests.
    - (4) Motivate employees to develop and maintain security consciousness.
    - (5) Assure that classified information and special nuclear material are adequately protected at all times.
    - (6) Assure that employees understand the full extent of their security responsibilities under Federal statutes, Executive Orders, and DOE Orders.

8211040154 821018  
PDR ADOCK 05000537  
A PDR

DISTRIBUTION:  
All Departmental Elements  
Federal Energy Regulatory Commission

INITIATED BY:  
Office of Safeguards  
and Security

- (7) Achieve maximum protection regarding all matters affecting the national security.
- b. Employees shall participate in the DOE safeguards and security awareness program, which covers such areas as the requirements for protecting classified information and special nuclear materials, and the obligation of employees to implement such requirements:
  - (1) Before being granted access to classified information or access or control over the access to special nuclear material.
  - (2) Periodically during the course of their employment.
  - (3) Upon termination of their access authorization or access to special nuclear material.

#### 4. REFERENCES.

- a. Atomic Energy Act of 1954, as amended, Section 141. Establishes policy of controlling the dissemination and declassification of Restricted Data.
- b. Executive Order 12065. Establishes the requirement for a security education program for agency and other personnel who have access to National Security Information.

#### 5. DEFINITIONS.

- a. Classified Information. (1) Restricted Data; (2) Formerly Restricted Data; or (3) National Security Information determined by appropriate authority, in accordance with Executive Order 12065 or other pertinent Executive Orders, to require protection against unauthorized disclosure in the interest of national security. Such information is designated with one of the three classification levels: Top Secret, Secret, and Confidential.
- b. Employees. Unless otherwise indicated, the word "employees", as used in this Order, refers to: DOE employees, consultants, assignees, and advisory board members; DOE contractor and subcontractor employees and consultants; and DOE access permittees.
- c. Formerly Restricted Data. Classified information jointly determined by the Department of Energy (or its predecessors) and the Department of Defense to be related primarily to the military utilization of atomic weapons, and removed by the DOE from the Restricted Data category pursuant to section 142(d) of the Atomic Energy Act of 1954, as amended, and safeguarded as National Security Information, subject to the restrictions on transmission to other countries and regional defense organizations that apply to Restricted Data.

- d. National Security Information. Information which requires protection in the interest of national defense or foreign relations of the United States, which is classified in accordance with an Executive Order, and which does not fall within the definition of Restricted Data or Formerly Restricted Data.
- e. Restricted Data. That data which is defined in Section 11(y) of the Atomic Energy Act of 1954, as amended, as "all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to Section 142."
- f. Safeguards and Security Awareness Program. A continuing, comprehensive campaign, incorporating modern instructional methods and communication techniques, designed to acquaint employees with their security responsibilities and to promote their compliance with applicable regulations.
- g. Special Nuclear Material. That material which is defined in Section 11(aa) of the Atomic Energy Act of 1954, as amended, as (1) plutonium, uranium, enriched in the isotope 233 or in the isotope 235, and any other material which pursuant to Section 51 of the Act has been determined to be special nuclear material, but not including source material; or (2) any material artificially enriched by any of the foregoing, but not including source material.

6. RESPONSIBILITIES AND AUTHORITIES.

- a. The Director of Safeguards and Security shall:
  - (1) Develop objectives, policy, standards, procedures, and guides for the DOE safeguards and security awareness program.
  - (2) Coordinate security education-related training of DOE personnel with other government agencies.
  - (3) Supply training aids and instructional material of broad application to DOE organizational elements.
  - (4) Evaluate effectiveness of security education and training throughout DOE and its contractors.
  - (5) Conduct periodic security education and training workshops at field offices and Headquarters.

- (6) Provide guidance in the policy interpretation of DOE safeguards and security awareness program requirements.
  - (7) Approve substantial deviations from prescribed security education schedules.
  - (8) For the Headquarters office (including DOE Regional Offices, the Energy Technology Centers, Power Marketing Administrations (except the Bonneville Power Administration), the Federal Energy Regulatory Commission, and the Environmental Measurements Laboratory):
    - (a) Establish and maintain a safeguards and security awareness program for DOE employees.
    - (b) Assure, through the contracting officer, that contractors establish and maintain safeguards and security awareness programs.
    - (c) Advise and assist Heads of Departmental Elements and the Chairman of FERC in conducting an on-the-job safeguards and security awareness program.
    - (d) When necessary, provide instruction in DOE security program and requirements to DOE and contractor employees who do not require access to classified information.
- b. Heads of Departmental Elements and Chairman, FERC shall:
- (1) Inform principal staff members of their security responsibilities, and require them to participate personally in the safeguards and security awareness program.
  - (2) Assure that subordinate supervisors are informed of and implement their responsibility for providing on-the-job security instructions to employees under their supervision.
- c. Managers of Field Organizations (Albuquerque, Chicago, Idaho, Nevada, Oak Ridge, Pittsburgh Naval Reactors, Richland, San Francisco, Savannah River, and Schenectady Naval Reactors) and the Assistant Administrator for Management Services, Bonneville Power Administration shall:
- (1) Establish and maintain a safeguards and security awareness program for DOE employees and consultants under their jurisdiction pursuant to the provisions of this Order.
  - (2) Assure, through the contracting officer, that contractors and subcontractors and their consultants and access permittees establish

and maintain safeguards and security awareness programs in accordance with the provisions of this Order.

- (3) When necessary, provide instruction in DOE security program and requirements to DOE and contractor employees who do not require access to classified information.



A handwritten signature in black ink, appearing to read "John C. Sawhill".

John C. Sawhill  
Deputy Secretary

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

ORDER

DOE 5631.2

11-13-80

SUBJECT: PERSONNEL SECURITY PROGRAM

- 
1. PURPOSE. To implement the provisions of the Atomic Energy Act of 1954, as amended, and Executive Orders 10450, 10865, and 12065.
  2. CANCELLATION. Interim Management Directive No. 6101, PERSONNEL SECURITY PROGRAM, of 9-29-77.
  3. SCOPE. The provisions of this Order apply to all Departmental elements, including the Federal Energy Regulatory Commission.
  4. BACKGROUND. The Personnel Security Program of the Department of Energy applies to its employees and contractors, as follows:
    - a. The provisions of the Atomic Energy Act of 1954, as amended, Executive Orders 10450 and 12065, and Federal Personnel Manual chapter 732 apply to Departmental employees, applicants for employment, consultants, employees of other Federal agencies, and assignees for employment and access; and
    - b. The provisions of the Atomic Energy Act of 1954, as amended, and Executive Orders 10865 and 12065 apply to Departmental contractors, subcontractor employees and consultants, and access permittees for access.
  5. REFERENCES.
    - a. Atomic Energy Act of 1954, as amended, Section 143, "Department of Defense Participation," Section 145, "Restrictions," and Section 161.b, "General Provisions," which are the legislative requirements for establishment of a DOE security program for controlling access to Restricted Data and special nuclear material.
    - b. 10 CFR Part 710, "Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Significant Quantities of Special Nuclear Material," as published in the "Federal Register", Vol. 42, No. 190, of 9-30-77, which is used in those cases in which there are questions of eligibility for DOE access.
    - c. DOE 1360.2, COMPUTER SECURITY PROGRAM FOR UNCLASSIFIED COMPUTER SYSTEMS, of 3-9-79, which established policies and procedures for developing, implementing, and administering a program for safeguarding DOE computer systems and in particular, DOE sensitive unclassified information.

---

DISTRIBUTION:  
All Departmental Elements  
Federal Energy Regulatory Commission

INITIATED BY:  
Office of Safeguards  
and Security

11-13-80

- d. Executive Order 10450, of 4-27-53, as amended, which established the requirement for determining that all Federal employees be loyal, reliable, trustworthy, and of good conduct and character.
  - e. Executive Order 10865, of 2-24-60, as amended which established the basis for industrial security program for civilian personnel.
  - f. Executive Order 12065, of 12-1-78, which established the restriction for access to classified information.
  - g. Federal Personnel Manual, Chapter 731, "Suitability," which contains requirements for employment by the Government regarding the character, reputation, and fitness of the individual under consideration.
  - h. Federal Personnel Manual, Chapter 732, "Personnel Security Program," which implements Executive Order 10450 throughout Federal departments and agencies.
  - i. Federal Personnel Manual, Chapter 736, "Investigations," which deals primarily with national agency checks and inquiries (NACI) and full field investigations conducted by the Office of Personnel Management.
  - j. Federal Personnel Manual Letter 732-7, "Personnel Security Program for Position Associated with Federal Computer Systems," which establishes policy for a personnel security program covering positions that are involved in the design, storage, retrieval, access, and dissemination of information maintained in Federal computer systems, as well as positions associated with automated decisionmaking systems.
  - k. Office of Management and Budget Circular No. A-71, "Security of Federal Automated Information Systems," of 7-27-78, with Transmittal No. 1, which promulgates policy and responsibilities for the development and implementation of computer security programs by executive branch departments and agencies.
6. IMPLEMENTATION. Additional implementation procedures will be published as necessary as extra chapters. These chapters will be coordinated separately.



William S. Heffelfinger  
Director of Administration

TABLE OF CONTENTS

	<u>PAGE</u>
<u>CHAPTER I - DEFINITIONS</u>	
1. Access .....	I-1
2. Access Authorization or Security Clearance .....	I-1
3. Access Permittee .....	I-2
4. Classified Information .....	I-2
5. Derogatory Information .....	I-2
6. Formerly Restricted Data .....	I-3
7. Hearing Counsel .....	I-3
8. Interim Access Authorization .....	I-3
9. National Security Information .....	I-3
10. Naval Nuclear Propulsion Information .....	I-3
11. Personnel Security Board .....	I-3
12. Position Sensitivity Designation .....	I-3
13. Restricted Data .....	I-3
14. Security Area .....	I-4
15. Sensitive Data .....	I-4
16. Sensitive Position .....	I-4
17. Special Nuclear Material .....	I-4
 <u>CHAPTER II - RESPONSIBILITIES AND AUTHORITIES</u>	
1. The Secretary .....	II-1
2. The Assistant Secretary for Defense Programs .....	II-1
3. Heads of Departmental Elements and Chairman, Federal Energy Regulatory Commission .....	II-2
4. General Counsel .....	II-2
5. Heads of Headquarters Elements .....	II-2
6. Director of Personnel .....	II-3
7. Director of Safeguards and Security .....	II-3
8. Heads of Field Organizations .....	II-5
 <u>CHAPTER III - POSITION SENSITIVITY DESIGNATIONS</u>	
1. General .....	III-1
2. Categories .....	III-1
a. Department of Energy Employees, Applicants for Employment, Consultants, and Assignees .....	III-1
b. DOE Contractor and Subcontractor Employees and Consultants and Access Permittees .....	III-3
c. Other Federal Department or Agency Employees .....	III-4



3. Sensitive Compartmented Information ..... III-5  
4. General Guidelines ..... III-5

CHAPTER I  
DEFINITIONS

1. ACCESS.

- a. The knowledge, use, or possession of classified information or other sensitive information not protected by National Security regulations which is required by an individual in the performance of official duties and which is provided to the individual on a "need-to-know" basis; or
- b. Situations involving the responsibilities of an individual in the performance of official duties which may provide proximity to or control over special nuclear material in Category I or II quantities.

2. ACCESS AUTHORIZATION OR SECURITY CLEARANCE. An administrative determination that an individual who is either a DOE employee, applicant for employment, consultant, assignee, other federal department or agency employee (and other persons who may be designated by the Secretary of Energy) or, a DOE contractor or subcontractor employee, is eligible for access to Restricted Data, other classified information, or special nuclear material. Clearances granted by the DOE are designated as "Q," "L," "Top Secret," or "Secret."

- a. "Q" access authorizations or clearances are based upon full field investigations conducted by the Federal Bureau of Investigation, Office of Personnel Management, or another Government agency which conducts personnel security investigations. They permit an individual to have access, on a "need-to-know" basis, to Top Secret, Secret and Confidential Restricted Data, Formerly Restricted Data, National Security Information, or special nuclear material in Category I or II quantities as required in the performance of duties. When "Q" access authorizations or clearances are granted to employees of access permit holders they are identified as "Q(X)" access authorizations or clearances and permit access only to the type of Secret Restricted Data specified in the permit.
- b. Top Secret access authorizations or clearances are based upon full field investigations conducted by the Office of Personnel Management or another Government agency which conducts personnel security investigations. They permit an individual to have access, on a "need-to-know" basis, to Top Secret, Secret, Confidential National Security Information, and Formerly Restricted Data as required in the performance of duties.
- c. "L" access authorizations or clearances are based upon National Agency Checks and Inquiries (NACI) for Federal employees, or National Agency Checks (NAC) for non-Federal employees, conducted by the Office of

Personnel Management. They permit an individual access, on a "need-to-know" basis, to Confidential Restricted Data, Secret and Confidential, Formerly Restricted Data, or Secret, and Confidential National Security Information, required in the performance of duties, provided such information is not designated "CRYPTO" (classified cryptographic information), other classified communications security ("COMSEC") information, or intelligence information. When "L" access authorizations or clearances are granted to employees of permit holders, they are identified as "L(X)" access authorizations or clearances and permit access only to the type of Confidential Restricted Data specified in the access permit. Additionally, the cognizant DOE official may grant an "L" access authorization or clearance to craft or manual workers, community management and service personnel, nurses, medical technicians, cafeteria workers, health and safety workers, purchasing and accounting groups, and the like, who are employed in classified construction or operations areas; provided the work of such individuals do not afford them:

- (1) More than visual access to buildings and equipment classified not higher than Secret Restricted Data; or
- (2) Access to information classified higher than Confidential Restricted Data concerning plant operating characteristics, process data, weapons, or weapons components.

d. Secret access authorizations or clearances are based upon National Agency Checks and Inquiries (NACI) for Federal employees, or National Agency Checks (NAC) for non-Federal employees, conducted by the Office of Personnel Management. They permit an individual access on a "need-to-know" basis, to Secret and Confidential National Security Information as required in the performance of duties.

3. ACCESS PERMITTEE. An individual or organization which has been issued a permit by the Department of Energy, providing access to Restricted Data applicable to civil uses of atomic energy in accordance with the terms and conditions stated on the permit and in accordance with applicable security regulations.
4. CLASSIFIED INFORMATION. Any information which requires protection against unauthorized disclosure in the interests of the national defense and security or foreign relations of the United States pursuant to U.S. Statute or Executive order. The term includes Restricted Data, Formerly Restricted Data, and National Security Information, each of which has degrees of importance denoted by the classifications Top Secret, Secret, or Confidential.
5. DEROGATORY INFORMATION. Unfavorable information concerning an individual which creates a question as to the individual's eligibility or continued eligibility for access or employment.

6. FORMERLY RESTRICTED DATA. Classified information jointly determined by the Department of Energy (or its predecessors, the Atomic Energy Commission and the Energy Research and Development Administration) and the Department of Defense to be related primarily to the military utilization of atomic weapons, and removed by the DOE from the Restricted Data category pursuant to section 142(d) of the Atomic Energy Act of 1954, as amended, and safeguarded as National Security Information, subject to the restrictions on transmission to other countries and regional defense organizations that apply to Restricted Data.
7. HEARING COUNSEL. A DOE attorney assigned to prepare and conduct Personnel Security Board Hearings.
8. INTERIM ACCESS AUTHORIZATION. A determination by the Secretary, for access to National Security Information, or by the Assistant Secretary for Defense Programs, for access to Restricted Data, that it is clearly consistent with the national interest for the DOE to permit an individual to have such access prior to the DOE's receipt of full field reports of investigation. Interim Access Authorizations are not processed for Access Permittees or for those individuals whose accesses will require an "L" or Secret clearance.
9. NATIONAL SECURITY INFORMATION. Information which requires protection in the interest of national defense or foreign relations of the United States and classified in accordance with an Executive order which does not fall within the definition of Restricted Data or Formerly Restricted Data.
10. NAVAL NUCLEAR PROPULSION INFORMATION. All information classified or unclassified concerning the design, arrangement, development, manufacture, testing, operation, administration, training, maintenance, and repair of the propulsion plants of naval nuclear powered ships, including the associated nuclear support facilities.
11. PERSONNEL SECURITY BOARD. A board appointed by the Head of a Field Organization to make findings and recommendations in granting access authorization to an individual which consists of three members, one of whom shall be designated chairperson.
12. POSITION SENSITIVITY DESIGNATION. A written certification by the appropriate DOE official that a position under his or her jurisdiction (to be occupied by a DOE employee, applicant for employment, consultant, or assignee) is critical-sensitive, noncritical-sensitive, or nonsensitive.
13. RESTRICTED DATA. Data which is defined in section IIy of the Atomic Energy Act of 1954, as amended, as "all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but

shall not include data declassified or removed from the Restricted Data category pursuant to section 142."

14. SECURITY AREA. A physically defined space containing classified matter (documents or material) or special nuclear materials subject to physical protection and personnel access controls.
15. SENSITIVE DATA. Information requiring a degree of protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data (e.g., personal data, proprietary data, sensitive energy data, sensitive financial or supply data, and so forth).
16. SENSITIVE POSITION. Any position in the DOE affected by, connected with, or related to the national security or welfare; i.e., a position whose occupant could, by virtue of the nature of such a position, bring about a materially adverse affect on the national security as prescribed in Executive Order 10450 and the Atomic Energy Act of 1954, as amended.
17. SPECIAL NUCLEAR MATERIAL. Special nuclear material, as defined in section II.aa of the Atomic Energy Act of 1954, as amended, not subject to a Nuclear Regulatory Commission license. For the purpose of this Order, special nuclear material in one facility or shipment is divided into the following categories:
  - a. Category "I" Quantities of SNM.
    - (1) Uranium 235 (contained in Uranium enriched to 20 percent or more in the isotope U-235) alone, or in combination with Plutonium and Uranium 233 when (multiplying the Plutonium and Uranium 233 content by 2.5) the total is 5,000 grams or more.
    - (2) Plutonium and Uranium 233 when the Plutonium and Uranium 233 content is 2,000 grams or more.
    - (3) SNM in lesser quantities but which is located in the same area or shipment with other SNM with which it could be selectively combined to produce the equivalent quantities in Items (a) or (b) of this category.
  - b. Category "II" Quantities of SNM.
    - (1) Uranium 235 (contained in Uranium enriched to 20 percent or more in the isotope U-235) alone, or in combination with Plutonium and Uranium 233 (multiplying the Plutonium and/or Uranium 233 content by 2.5) when the total is 1,000 to 4,999 grams.

- (2) Plutonium and Uranium 233 when the Plutonium and Uranium 233 content is 400 grams to 1,999 grams.
- (3) SNM in lesser quantities but which is located in the same area or shipment with other SNM with which it could be selectively combined to produce the equivalent quantities in subparagraphs (1) or (2) of this category.

CHAPTER II

RESPONSIBILITIES AND AUTHORITIES

1. THE SECRETARY shall:

- a. Certify those specific positions which are of a high degree of importance or sensitivity under section 245f of the Atomic Energy Act of 1954, as amended, which are to be subject of an investigation by the Federal Bureau of Investigation.
- b. Designate those specific positions within DOE which are sensitive under section 3(b) of Executive Order 10450.
- c. Authorize, in the case of emergency, and for a limited period of time, a sensitive position (including either critical-sensitive or noncritical-sensitive) to be occupied within the DOE by an individual for whom a preappointment full field investigation has not been completed, if such action is necessary in the national interest under section 3(b) of Executive Order 10450.
- d. Grant authorization for access to National Security Information pursuant to section 4-201 of Executive Order 12065 prior to completion of the required investigation when it has been determined that such action is in the national interest.
- e. Establish standards and specifications in writing as to the scope and extent of investigations under section 145g of the Atomic Energy Act of 1954, as amended.
- f. Make determinations required by 10 CFR part 710.27(m)(2)(ii) and 10 CFR part 710.33.

2. THE ASSISTANT SECRETARY FOR DEFENSE PROGRAMS shall:

- a. Grant authorization for access to Restricted Data pursuant to Section 145b of the Atomic Energy Act of 1954, as amended, prior to completion of the required investigation when he has determined that such action is in the national interest.
- b. Direct the suspension of access authorization in accordance with 10 CFR part 710.21.
- c. Issue subpoenas to witnesses in all cases processed in accordance with 10 CFR part 710.20 et seq.

- d. Act as "special designee" under 10 CFR part 710.27(m)(2)(j) to determine whether statements may be received by Personnel Security Boards and determine whether new evidence may be received in accordance with 10 CFR part 710.29(b)(2).
  - e. Submit records in Administrative Review proceedings in accordance with 10 CFR part 710.30(d)(2) and (e).
  - f. Grant, deny, or revoke access authorization in accordance with 10 CFR part 710.24(a) and 710.32.
  - g. Approve reconsideration of access authorization cases in accordance with 10 CFR part 710.34.
  - h. Select and appoint the individuals who offer findings and recommendations in administrative review cases in accordance with 10 CFR part 710.31.
3. HEADS OF DEPARTMENTAL ELEMENTS AND CHAIRMAN, FEDERAL ENERGY REGULATORY COMMISSION shall:
- a. Generate requests to the Secretary for waivers of preappointment full field investigation requirement for candidates under consideration to occupy a critical-sensitive position which does not require access to Restricted Data.
  - b. Generate requests to the Secretary or the Assistant Secretary for Defense Programs, through the Director of Safeguards and Security, for Interim Access Authorizations.
4. GENERAL COUNSEL shall:
- a. Approve notification letters to individuals whose eligibility for access authorization is in question in accordance with 10 CFR part 710.22.
  - b. Concur in request for issuance of subpoenas to witnesses in cases processed in accordance with 10 CFR part 710.20 et seq.
  - c. Concur in request for suspensions in cases processed in accordance with 10 CFR part 710.21.
5. HEADS OF HEADQUARTERS ELEMENTS shall:
- a. Certify, in writing to the Director of Personnel, Position Sensitivity Designations for each position under their jurisdiction to be occupied by a DOE employee or applicant for employment, consultant, or assignee.



- b. Approve and transmit to the Director of Safeguards and Security, Headquarters, requests for access authorization of employees of other Federal departments or agencies who require access to Restricted Data.
  - c. Approve and transmit to the Director of Safeguards and Security, Headquarters, applications for access authorizations for foreign nationals.
  - d. Furnish Data Report on Spouse (DOE Form DP-354) for personnel under their jurisdiction who possess an access authorization.
  - e. Approve and transmit to the Director of Safeguards and Security, Headquarters, requests for access authorizations for members of the Armed Forces and civilian employees of the Department of Defense and the National Aeronautics and Space Administration assigned to duty with DOE Headquarters organizations, for access to Restricted Data.
6. HEADQUARTERS, DIRECTOR OF PERSONNEL shall:
- a. Receive position sensitivity designations for Headquarters positions and provide copies of certifications to the Director of Safeguards and Security, Headquarters.
  - b. Process all requests for investigations for DOE Headquarters employees, applicants for employment, consultants, and assignees to the Director of Safeguards and Security, Headquarters.
  - c. Determine final action to be taken in those cases where questionable suitability information is developed.
7. HEADQUARTERS, DIRECTOR OF SAFEGUARDS AND SECURITY shall:
- a. Develop policy, objectives, standards, guides, and procedures for the DOE Personnel Security Program.
  - b. Authorize Heads of Field Organizations to initiate security investigations relative to foreign nationals who are applicants for security clearance.
  - c. For cases processed in accordance with the provisions of 10 CFR part 710.20 et seq. and 10 CFR part 710.38, perform the functions assigned to the Director of Safeguards and Security, Headquarters, and make recommendations to the Assistant Secretary for Defense Programs as appropriate.
  - d. Process all requests by other Government agencies for verification of an individual's DOE security clearance status.

- e. Maintain centralized records for all DOE security clearance actions.
- f. Coordinate requests by the Inspector General for access to personnel security information for investigative purposes.
- g. For Headquarters, approve and maintain records of review of personnel security files by properly identified employees of investigative agencies of the Federal Government and other routine users under Privacy Act regulations.
- h. Recommend to the Controller funding necessary for conducting personnel security investigations.
- i. Maintain liaison with the Federal Bureau of Investigation and the Office of Personnel Management and is principal point of contact with these agencies on all personnel security matters.
- j. Notify the Federal Bureau of Investigation or Office of Personnel Management of withdrawals of requests for investigation.
- k. Initiate:
  - (1) Investigation of spouses of individuals who marry after having been processed for an access authorization.
  - (2) Appropriate investigation and grant access authorizations for access to Restricted Data for:
    - (a) Personnel of the Department of Defense (DOD) and the National Aeronautics and Space Administration (NASA) assigned for duty with DOE or DOE contractors or with other Federal departments or agencies, and
    - (b) Employees of other Federal departments or agencies who require such access.
- l. Accept properly executed certifications for DOD and NASA personnel assigned for duty with DOE who require access to Restricted Data.
- m. Concur in requests to the Secretary for waivers of preappointment full field investigation requirements for candidates under consideration to occupy critical-sensitive positions not requiring a "Q" clearance.
- n. Accept properly executed requests for Interim Access Authorizations; conduct appropriate indices checks and forward such requests to the Assistant Secretary for Defense Programs with appropriate recommendations.

- o. For DOE Headquarters (including Grand Junction Office, DOE regional offices, energy technology centers, power marketing agencies, (except the Bonneville Power Administration), Federal Energy Regulatory Commission, Strategic Petroleum Reserves Office, and the Environmental Measurements Laboratory):
  - (1) Implement the Personnel Security Program consistent with the objectives, standards, guides, and procedures stated in this Order and in 10 CFR part 710.
  - (2) Perform functions listed on pages II-5 through II-7, subparagraphs 8b, d, e, f, g, and k.
  - (3) Perform functions listed on pages II-7 and II-8, subparagraph 8m(1) through (5), (8), (9), and (10).
  - (4) Make an annual compilation of "Positions of a High Degree of Importance or Sensitivity" for certification.
  - (5) Process Data Reports on Spouse (DOE Form DP-354).
  - (6) Process cases of DOE or DOE contractor personnel who are hospitalized or otherwise treated for a mental illness which may cause a defect in judgment or reliability.
  - (7) Evaluate all reports of investigation conducted on DOE employees and applicants for employment for suitability in sensitive positions, and notify the Director of Personnel, Headquarters, of the results of each investigation for appropriate action.
8. HEADS OF FIELD ORGANIZATIONS, INCLUDING PITTSBURGH NAVAL REACTORS, SCHENECTADY NAVAL REACTORS AND THE ASSISTANT ADMINISTRATOR FOR MANAGEMENT SERVICES, BONNEVILLE POWER ADMINISTRATION (EXCLUDING THOSE ORGANIZATIONS MENTIONED ON PAGE II-5, SUBPARAGRAPH 7o), ALBUQUERQUE, CHICAGO, IDAHO, NEVADA, OAK RIDGE, RICHLAND, SAN FRANCISCO, SAVANNAH RIVER shall:
  - a. Implement the Personnel Security Program consistent with the policy, objectives, standards, guides, and procedures stated in this Order and in 10 CFR part 710.
  - b. Initiate requests for investigation directly to the Federal Bureau of Investigation or Office of Personnel Management.
  - c. Determine the position sensitivity and access requirements prior to requesting investigations for DOE employees or applicants for employment, consultants, and assignees.

- d. Determine the access requirements prior to requesting investigations for DOE contractor or subcontractor employees, consultants, or access permittees.
- e. Implement procedures which require DOE supervisors and DOE contractor organizations to report information received that an individual under their jurisdiction, possessing an active access authorization, is hospitalized or otherwise treated for a mental illness which may cause a defect in judgment or reliability, and to notify the Director of Safeguards and Security, Headquarters, of this fact and when such employee is found to be free of such defect.
- f. Arrange for the service of a psychiatrist to examine an individual when such an examination is determined appropriate in resolving a question of eligibility for access authorization, or continuing access authorization.
- g. Implement procedures under a supervisory security program to assure that DOE supervisors and DOE contractor organizations are aware that:
  - (1) Information concerning an individual possessing an active DOE access authorization (or in process for same) that is a matter of personnel security interest should be reported to a DOE security official.
  - (2) Established reporting channels should be used in communicating a matter of personnel security concern to the appropriate DOE security official.
- h. Request approval of the Director of Safeguards and Security, Headquarters, to initiate security investigations relative to foreign nationals.
- i. Refer to the Director of Safeguards and Security, Headquarters, requests for access authorization for employees of other Federal departments and agencies.
- j. Furnish the Director of Safeguards and Security, Headquarters, with:
  - (1) Written notifications of withdrawals of requests for access authorizations.
  - (2) An annual compilation of "Positions of a High Degree of Importance or Sensitivity" for certification.
  - (3) Data Reports on Spouse (DOE Form DP-354) for personnel under their jurisdiction who marry subsequent to the processing for an access authorization.

- k. Accept for access to "Confidential" or "Secret" National Security Information (Non-Restricted Data) or Formerly Restricted Data involved in DOE contracts and subcontractors, written assurances that personnel of the facility engaged in DOE work possess final DOD or NASA clearances for access to national security information and the type of investigation on which such clearances were granted. Clearances granted by DOD contractors and interim "Confidential" or "Secret" clearances are not acceptable. Appropriate records of accepted clearances shall be maintained by the field organization.
- l. Generate requests to the Secretary or the Assistant Secretary for Defense Programs, through the Director of Safeguards and Security, Headquarters, for Interim Access Authorizations.
- m. In addition to the above, Heads of Field Organizations and the Assistant Administrator for Management Services, Bonneville Power Administration:
  - (1) Grant access authorization in all cases except those requiring processing for a Personnel Security Board hearing.
  - (2) Cause individuals to be interviewed when the reported information falls within the criteria of 10 CFR part 710 or Executive Order 10450.
  - (3) In connection with cases processed in accordance with 10 CFR part 710.20 et seq, perform those functions assigned to the Heads of Field Organizations.
  - (4) Extend, accept for transfer, reinstate, and terminate access authorizations as appropriate.
  - (5) Authorize transfer of contractor personnel, whose access authorizations are based upon investigations by the Office of Personnel Management or other Government agencies, to positions of a "High Degree of Importance or Sensitivity" prior to receipt of Federal Bureau of Investigation reports.
  - (6) Furnish the Director of Safeguards and Security, Headquarters, with appropriate notifications of all access authorization actions.
  - (7) Approve and maintain records of review of personnel security files by properly identified employees of investigative agencies of the Federal Government and other routine users under Privacy Act regulations.

- (8) Accept investigations and reports on the character, associations, and loyalty of individuals made by the Office of Personnel Management, Federal Bureau of Investigation, or another Government agency which conducts personnel security investigations, provided that a security clearance has been granted to such individuals by another Government agency based on such investigations and reports.
- (9) Maintain personnel security files, as appropriate, containing copies of reports of investigation and other pertinent data on individuals granted a DOE security clearance by that office, or where an investigation was requested by that office and reports of investigation forwarded by virtue of the fact that the individual occupied a critical-sensitive position.
- (10) Assure that the information reflected on standard employment forms completed by DOE employees, applicants for employment, consultants and assignees is comparable with the information reflected on security forms prior to the security forms being forwarded to the appropriate investigative agency.
- (11) Evaluate all applicable reports of investigation conducted on DOE employees and applicants for employment under their jurisdiction for suitability in sensitive positions and notify the cognizant office of the results of each investigation for appropriate action.

CHAPTER III

POSITION SENSITIVITY DESIGNATIONS

1. GENERAL. The position sensitivity designation for each category of personnel for employment and access are contained in this chapter. Sensitive compartmented information and general guidelines on requests for clearances are in paragraphs 3 and 4.
2. CATEGORIES.
  - a. Department of Energy (DOE) Employees, Applicants for Employment, Consultants, and Assignees.
    - (1) It is DOE policy to afford employment, and access to Restricted Data, National Security Information and other sensitive data not subject to National Security Regulations, and Category I or Category II quantities of special nuclear material to individuals concerning whom the DOE has made a determination that such employment and access will not endanger the common defense and security and is clearly consistent with the national interest. Except as authorized by the Secretary (or designee) that such action is clearly consistent with the national interest, this determination shall be based upon an investigation and report by the Office of Personnel Management, Federal Bureau of Investigation, or another Government agency which conducts personnel security investigations, provided (in those instances involving access to Restricted Data) that a security clearance has been granted to such individuals by another Government agency based on such an investigation and report.
    - (2) To assure that investigative coverage is appropriate for the individual's level of responsibility and access, a determination shall be made as to the sensitivity of each Departmental position and certified in writing to the Director at Headquarters, or to the appropriate DOE official at a DOE field office. This certification of Position Sensitivity Designation shall indicate whether the position is critical-sensitive, noncritical-sensitive, or nonsensitive; and if critical-sensitive or noncritical-sensitive, shall indicate which of the criteria in (a) or (b) below was used as a basis for that determination, and the degree of access (if any) which is involved. The following criteria shall be used in the determination of the Position Sensitivity Designation.
      - (a) Critical-Sensitive Position. A sensitive position, requiring a pre-appointment Office of Personnel Management full field investigation, the duties of which include any of the following:

- 1 Access to Top Secret National Security Information.
  - 2 Access to Secret Restricted Data.
  - 3 Access to Special Nuclear Material in Categories I or II.
  - 4 Access to, and development or approval of war plans or particulars of future or major or special operations of war, or critical or extremely important items of war.
  - 5 Access to, and development or approval of plans, policies, or programs which affect the overall operations of the DOE.
  - 6 Fiduciary, public contact, or other responsibilities demanding the highest degree of public trust.
  - 7 Responsibility for the planning, direction, and implementation of a computer security program; major responsibility for the direction, planning, and design of a computer system, including the hardware and software; or the capability to access a computer system during its operation or maintenance in such a way, and with a relatively high risk for causing grave damage, or realization of significant personal gain (ADP-1).
  - 8 Access to "CRYPTO" (classified cryptographic information) or other classified communications security (COMSEC).
- (b) In addition to the above criteria for determining critical-sensitive position designations, the following additional responsibilities or considerations shall be used to establish whether a critical-sensitive position is a "Position of a High Degree of Importance or Sensitivity" within the meaning of section 145f of the Atomic Energy Act of 1954, as amended, requiring a pre-appointment FBI full field investigation.
- 1 Regular access to Top Secret Restricted Data.
  - 2 Regular access to Restricted Data involving broad policy or program direction in any of the following:
    - a Research and development programs pertaining to nuclear or thermonuclear weapons or special nuclear material production.
    - b Production or stockpile of nuclear or thermonuclear weapons or special nuclear material.



- c Research, development, or production in the laser fusion or laser isotope programs.
            - d Naval nuclear propulsion program.
            - 3 Any other position so designated by the Secretary.
          - (c) Noncritical-Sensitive Position. A sensitive position, not within the categories described above, requiring a preappointment National Agency Check and Inquiry (NACI), the duties of which include any of the following:
            - 1 Access to Confidential Restricted Data.
            - 2 Access to Secret or Confidential National Security Information.
            - 3 Responsibility for the direction, planning, design, operation, and maintenance of a computer system, and whose work is technically reviewed by a higher authority in a critical-sensitive position to assure the integrity of the system (ADP-II).
          - (d) Nonsensitive Position. A position requiring a NACI but not requiring a clearance connected with, or relative to the national security or welfare, and which does not fall into any of the categories described above. This also includes all other positions involved in computer activities not specified on page III-2, paragraph 2a(2)(a)7 and page III-3, paragraph 2a(2)(c)3.
- b. DOE Contractor and Subcontractor Employees and Consultants, and Access Permittees.
  - (1) It is DOE policy to withhold the access to Restricted Data, other classified information, and quantities of special nuclear material of DOE contractor and subcontractor employees and consultants and access permittees until the DOE has made a determination that such access will not endanger the common defense and security. Except as authorized by the Secretary or his designee that such action is clearly consistent with the national security, this determination shall be made based upon an investigation and report by the Office of Personnel Management, Federal Bureau of Investigation, or another Government agency which conducts personnel security investigations, provided (in those instances involving access to Restricted Data) that a security clearance has been granted to such individual by another Government agency based on such an investigation and report.

- (2) To assure that investigative coverage is appropriate, the individual's type of access (Restricted Data, National Security Information, or unclassified Special Nuclear Material in Category I or II Quantities) and level of access (Top Secret, Secret, or Confidential) shall be determined before a request for investigation is made by the appropriate DOE official. Additionally, a DOE contractor or subcontractor employee or consultant position shall be designated as a "Position of a High Degree of Importance or Sensitivity" within the meaning of section 145f of the Atomic Energy Act of 1954, as amended, when the duties of that position include any of the following:
- (a) Regular access to Top Secret Restricted Data.
  - (b) Regular access to Restricted Data involving broad policy or program direction in any of the following:
    - 1 Research and development programs pertaining to nuclear or thermonuclear weapons or special nuclear material production.
    - 2 Production or stockpile of nuclear or thermonuclear weapons or special nuclear material.
    - 3 Research, development, or production in the laser fusion or laser isotope programs.
    - 4 Naval nuclear propulsion program.
- (3) It is DOE policy not to establish a separate clearance program for DOE contractor and subcontractor employees and consultants and access permittees for positions associated with unclassified Federal Computer Systems. Rather, the contractor, subcontractor, consultants, or access permittee is responsible for maintaining satisfactory standards of employees qualifications, performance, conduct, and business ethics under its own personnel policies (U.S. Department of Energy Procurement Regulation, Subpart 9-50.12, Labor Relations, 9-50.1201-2(a)).

c. Other Federal Department or Agency Employees.

- (1) It is DOE policy to withhold the access to Restricted Data, other classified information under DOE responsibility, and quantities of special nuclear material of other Federal employees until the DOE has made a determination that such access will not endanger the common defense and security. Except as authorized by the Secretary or his designee that such action is clearly consistent with the

national security, this determination shall be based upon an investigation and report by the Office of Personnel Management, Federal Bureau of Investigation, or another Government agency which conducts personnel security investigations provided (in those instances involving access to Restricted Data) that a security clearance has been granted to such individual based on such investigation and report.

- (2) Additionally, positions within other Federal departments (exclusive of personnel of the Department of Defense and the National Aeronautics and Space Administration, who do not require DOE security clearance by virtue of section 143 of the Atomic Energy Act of 1954, as amended, or section 304(b) of the National Aeronautics and Space Act of 1958) and agencies shall be designated as a "Position of a High Degree of Importance or Sensitivity" within the meaning of section 145f of the Atomic Energy Act of 1954, as amended, when the duties of that position include any of the following:
  - (a) Regular access to Top Secret Restricted Data.
  - (b) Regular access to Restricted Data involving broad policy or program direction in any of the following:
    - 1 Research and development programs pertaining to nuclear or thermonuclear weapons or special nuclear material production.
    - 2 Production or stockpile of nuclear or thermonuclear weapons or special nuclear material.
    - 3 Research, development, or production in the laser fusion or laser isotope separation programs.
    - 4 Naval nuclear propulsion program.
3. SENSITIVE COMPARTMENTED INFORMATION (SCI). Within the DOE, determinations concerning an individual's eligibility for access to SCI are the responsibility of the Senior Intelligence Officer and his or her designated representative(s). The granting of access to SCI shall be controlled under the strictest application of the "need-to-know" principle under procedures prescribed in Director of Central Intelligence Directive (DCID), No. 1/14.
4. GENERAL GUIDELINES. Requests for clearances shall be submitted only after a determination has been made that the duties of a position require access to classified information, or special nuclear material in Category I or II quantities, or regular access to a security area. Clearances are not to be requested as a means for alleviating individual or management responsibility to safeguard classified information properly or control dissemination of

such classified information on a "need-to-know" basis. It is the intent of this policy to assure that clearances are requested only when absolutely required to avoid the unnecessary expenditure of agency funds and resources or the unwarranted invasion of an individual's right to privacy.

- (1) The DOE will take all reasonable measures to obtain existing reports of investigation which may fulfill the agency standards and specifications as to the scope and extent of investigations established by the Secretary.
- (2) Requests for clearances will not be processed: (a) unless all required security forms are completed and signed (when appropriate) by the applicant; (b) if the printed content of the security forms has been altered; (c) if insufficient information is provided or the forms are illegible.
- (3) The possession of a DOE clearance permits an individual access to the levels of classified information (on a "need-to-know" basis) as shown below:

<u>Type Clearance</u>	<u>Access Permitted*</u>
DOE Employees, Applicants for employment, Consultants, and Assignees; and DOE Contractor and Subcontractor Employees and Consultants:	
"Q - Sensitive"	Top Secret RD, FRD, & NSI Secret RD, FRD, & NSI Confidential RD, FRD & NSI
"Q - Nonsensitive"	Top Secret NSI, & FRD Secret RD, FRD & NSI Confidential RD, FRD, & NSI
Top Secret	Top Secret NSI, & FRD Secret NSI, & FRD Confidential NSI & FRD
"L"	Secret NSI, & FRD Confidential RD, FRD, & NSI
Secret	Secret NSI, & FRD Confidential NSI, & FRD

Employees of DOE Access Permit Holders:

"Q(X)"

Secret RD  
Confidential RD  
(as specified in the  
access permit)

"L(X)"

Confidential RD  
(as specified in the  
access permit)

---

Other Federal Department/Agency Employees:

"Q - Sensitive"

Top Secret RD  
Secret RD  
Confidential RD

"Q - Nonsensitive"

Secret RD  
Confidential RD

"L"

Confidential RD

\*(RD - Restricted Data; FRD - Formerly Restricted Data; NSI - National Security Information)

# U.S. Department of Energy

Washington, D.C.

## ORDER

DOE 5631.3

2-3-81

SUBJECT: ISSUANCE AND CONTROL OF CREDENTIALS, SHIELDS, AND COURIER CARDS

1. PURPOSE. This Order establishes the Department of Energy (DOE) policy and procedures governing the issuance and control of credentials, shields, and courier cards.
2. CANCELLATION. Interim Management Directive 6109, Issuance and Control of Credentials, of 12-7-77.
3. SCOPE. The provisions of this Order are applicable to all Departmental Elements, including the Federal Energy Regulatory Commission.
4. POLICY. DOE credentials, shields, and courier cards will be issued only to authorized employees of DOE for whom such issuance is deemed necessary in the performance of their official duties.
5. BACKGROUND. The credential is a means of identification for DOE employees for use in the conduct of inspections, interviews, audits, interagency liaison, and similar type activities. The shield is a metal, police-type badge, which may be issued to an appropriate DOE-appointed security official for his or her everyday official use with local law enforcement officials for identification purposes only. It can be used along with the existing DOE credential. The shield does not provide any additional legal or law enforcement authority, and its misuse will result in immediate revocation. The courier card is a means of identification for DOE employees authorized to transport classified information or material between secure facilities. Where necessary, the courier card may authorize appropriate arming of employees of DOE in accordance with Section 161 k of the Atomic Energy Act of 1954, as amended, for the protection of material in their custody. This authority does not extend to the arming of noncourier escorts furnished by DOE contractors or other Government agencies.
6. RESPONSIBILITIES AND AUTHORITIES.
  - a. Director of Safeguards and Security.
    - (1) Administers the DOE credential, shield, and courier card programs.
    - (2) Approves the credential, shield, and courier card issuance to Headquarters employees whose duties require official identification

DISTRIBUTION:  
All Departmental Elements  
Federal Energy Regulatory Commission

INITIATED BY:  
Office of Safeguards  
and Security

pursuant to DOE Regulations, except for the Senior Intelligence Officer and the Inspector General who will issue credentials, shields, and courier cards to personnel under their cognizance.

- (3) Upon written request, provides the Senior Intelligence Officer, the Inspector General, or field organizations with blank credentials, blank courier cards, or shields to be issued to personnel under their cognizance.
  - (4) Maintains a register of accountability for all credentials, shields, and courier cards issued. (The record of credentials, shields, and courier cards forwarded to field organizations and the Inspector General and the Senior Intelligence Officer shall be maintained by block numbers).
- b. Heads of Departmental Elements, and Chairman, Federal Energy Regulatory Commission.
- (1) Assure that only those employees with an official need are issued credentials, shields, or courier cards, and that the credentials, shields, and courier cards are used for official purposes.
  - (2) Inspector General, the Senior Intelligence Officer, and all Departmental elements shall maintain a record showing disposition of all credentials, shields, and courier cards issued. The loss or recovery of credentials, shields, or courier cards shall be reported to the Headquarters Director of Safeguards and Security.
  - (3) Report any allegations of misuse to the issuing organization or to the Inspector General or to the Senior Intelligence Officer.
  - (4) Retrieve and destroy credentials and courier cards, and retrieve shields, when an employee terminates or transfers to a position where the credentials, shields, or cards are no longer required.
  - (5) The Albuquerque Operations Office shall design, issue, and control an appropriate identification card specifically for use by the Transportation Safeguards Division couriers.

c. Employees.

- (1) Use the credentials, shields, and courier cards only for official purposes.
- (2) Immediately report lost or stolen credentials, shields, or courier cards, with the details surrounding the circumstances, to the issuing organization.

7. PROCEDURES FOR THE ISSUANCE OF CREDENTIALS.

- a. Requests for approval of issuance of credentials shall be submitted, in the format shown in Attachment 1, to the Director of Safeguards and Security, the Inspector General, the Senior Intelligence Officer, or the field organization Director of Security, as appropriate.
- b. The issuing organizations shall take the following actions:
  - (1) The individual's name and title are entered in the appropriate spaces on the lower portion of the credential.
  - (2) The signature of the individual is inscribed in the appropriate block on the upper portion.
  - (3) The signature of the Director of Safeguards and Security, the Inspector General, the Senior Intelligence Officer, or field organization Director of Security, as appropriate, is affixed on each approved set. Facsimile signatures shall not be used.
  - (4) The photograph of the individual is affixed and the credentials are laminated and encased (a polaroid-type color photograph of good quality as suggested).
  - (5) Credentials will be given to the individual upon completion of the acknowledgment statement (Attachment 2). A shield may also be issued at this time, if deemed useful for identification purposes only.
  - (6) The acknowledgment statement will be retained by the Director of Safeguards and Security, the Inspector General, the Senior Intelligence Officer, or field organization Director of Security, as appropriate.
- c. Questions regarding this Order should be directed to the Management Support Staff, Office of Safeguards and Security, Washington, D.C., 20545.

8. PROCEDURES FOR THE ISSUANCE OF COURIER CARDS. In all cases where authorization for appropriate arming is necessary, requests for the issuance of courier cards shall be submitted to the Director of Safeguards and Security as shown below:

a. Headquarters.

- (1) The Administrative Officer of the Office of Administrative Services forwards a memorandum to the Director of Safeguards and Security for



a courier card and provides appropriate documentation showing that the individual to be issued a courier card possesses the necessary degree of expertise in operating and maintaining any and all weapons to be used. Such documentation may take the form of a firearms qualification record prepared in accordance with accepted military or law enforcement practices, or other forms as provided for or approved by the Director of Safeguards and Security.

- (2) The Office of Safeguards and Security checks that the individual is "Q" cleared, determines whether the documented degree of expertise in operating and maintaining weapons is adequate, and prepares the courier card.
- (3) The Office of Safeguards and Security issues the courier card to the individual with an acknowledgment card which must be signed by the individual and returned to the Management Support Staff of the Office of Safeguards and Security.

b. Field Organizations. Directors of Security of field organizations shall:

- (1) Request courier cards by memorandum to the Headquarters Director of Safeguards and Security and return signed acknowledgment forms on receipt of the cards. The cards may be issued in blocks of one hundred or more.
- (2) Establish similar procedure for issuance of cards indicated on page 3, paragraph 8a.

9. EXAMPLES. Examples of credentials and courier cards are attached.



William S. Heffelfinger  
Director of Administration



Department of Energy  
Washington, D.C. 20545

TO : Director, Safeguards and Security  
Department of Energy

FROM : Chief, Weapons Division

SUBJECT: REQUEST FOR CREDENTIALS

Credential authorization is hereby requested for the below noted employee of DoE. Authorization is required in connection with the individual's duties pursuant to DoE Regulations.

1. Name: Robert E. Green

2. Title: Research Specialist

3. Organization: Weapons Division

10-20-80 John R. Green  
Date of Request Signature of Requesting Official

APPROVED: Steve Smith 10-30-80  
Signature, Director Date  
Safeguards and Security

DISAPPROVED: \_\_\_\_\_  
Signature, Director Date  
Safeguards and Security

Reason for Disapproval: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

EXAMPLE

CREDENTIAL ACKNOWLEDGMENT STATEMENT

I, Robert E. Green, acknowledge receipt of DOE Credential Number 2443. I understand that it is to be used only in the performance of my official duties at the Department of Energy, Reference Title 18, Section 499, United States Code. In the event I am reassigned, transferred, terminated, or otherwise no longer require this credential, I will surrender the credential to the issuing office.

11-5-80  
Date

E. Green  
Signature

EXAMPLE

DOE F 1326.2  
(7-79)

U.S. DEPARTMENT OF ENERGY  
**memorandum**

DATE 10-15-80

REPLY TO  
ATTN OF DP-312

SUBJECT DEPARTMENT OF ENERGY COURIER CARD INSERTS

TO (Requesting Official)

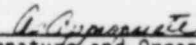
In accordance with your recent request, there are enclosed 100 copies of DOE Courier Identification inserts, numbers 0785 through 0884.

Please sign, date and return to this office the receipt shown at the bottom of this memorandum.

  
James P. Weeks  
Chief, Management Support Staff  
Office of Safeguards and Security

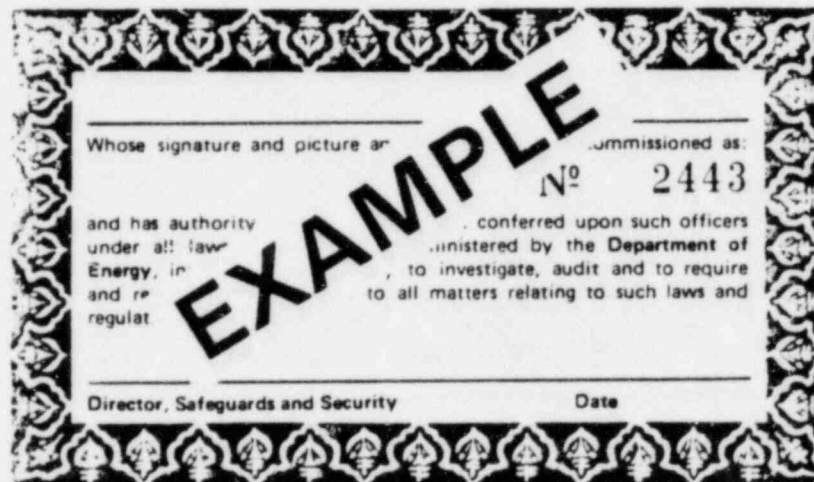
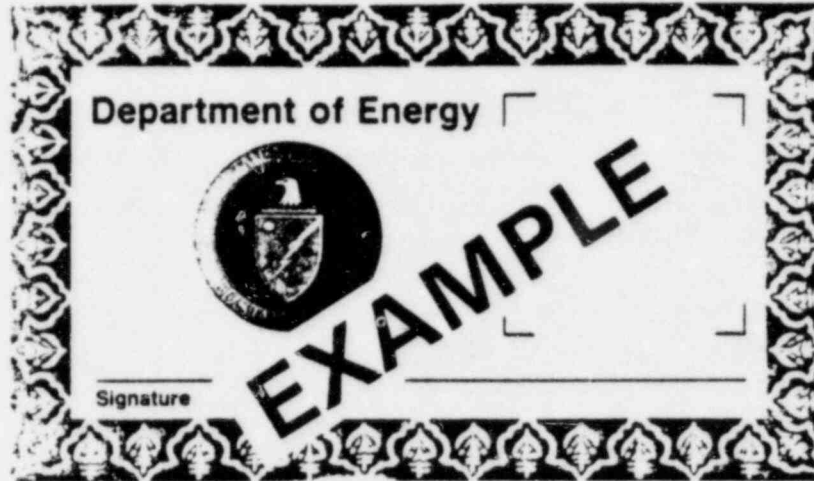
Enclosures:  
Courier Identification Inserts

-----  
I have received the Courier Identification inserts referenced above,  
numbers 0785 through 0884.

  
\_\_\_\_\_  
(Signature and Organization Title)

\_\_\_\_\_  
10-22-80  
(Date)

DOE CREDENTIAL



DOE COURIER CARD

**UNITED STATES  
DEPARTMENT OF ENERGY  
WASHINGTON, D**

THIS IS TO CERTIFY

WHOSE SIGNATURE, PHOTOGRAPH, AND PHYSICAL DESCRIPTION APPEAR BELOW IS THAT OF A QUALIFIED OFFICER OF THE UNITED STATES DEPARTMENT OF ENERGY AND, AS SUCH, IS AUTHORIZED TO PERFORM FUNCTIONS UNDER SECTION 161.K OF THE ATOMIC ENERGY ACT OF 1954, AS AMENDED, TO BEAR FIREARMS IN THE PERFORMANCE OF HIS OFFICIAL DUTIES. HE IS AUTHORIZED TO ACCESS RESTRICTED DATA AND OTHER CLASSIFIED INFORMATION.

**EXAMPLE**

No. 0785

DATE OF BIRTH:  
HEIGHT:  
HAIR COLOR:  
WEIGHT:  
EYE COLOR:

**EXAMPLE**

SIGNATURE \_\_\_\_\_

DIRECTOR OF SAFEGUARDS & SECURITY

No. 0785

DOE COURIER CARD  
TRANSPORTATION SAFEGUARDS DIVISION  
ALBUQUERQUE OPERATIONS OFFICE

<p><b>FEDERAL OFFICER</b> U.S. DEPARTMENT OF ENERGY ALBUQUERQUE</p> <p>THE PERSON IDENTIFIED HEREON IS A COURIER OF THE U.S. DEPARTMENT OF ENERGY AND IS AUTHORIZED TO CARRY FIREARMS IN THE PERFORMANCE OF OFFICIAL ASSIGNMENTS.</p> <p>0283</p> <p>AL-190 (10-77) DOE ALO</p>
---

DOB	WT	HT	HAIR	EYES
COURIER'S SIGNATURE _____				
THE PERSON IDENTIFIED HEREON, A COURIER OF THE USDOE ASSIGNED TO THE TRANSPORTATION SAFEGUARDS DIVISION OF THE ALBUQUERQUE OPERATIONS OFFICE, ALBUQUERQUE, NEW MEXICO, IS AUTHORIZED TO CARRY FIREARMS, PURSUANT TO PUBLIC LAW 93-703, IN THE PERFORMANCE OF OFFICIAL ASSIGNMENTS AND TO PROTECT THE MATTER IN CUSTODY BY THE USE THEREOF. REVEALING THE NATURE OR CONTENTS OF SUCH MATTER TO ANYONE EXCEPT DULY AUTHORIZED PERSONS IS PROHIBITED. ANY PERSON WHO, WITHOUT PROPER AUTHORITY FROM THE USDOE, ACQUIRES OR EXAMINES ANY RESTRICTED DATA OR OTHER CLASSIFIED MATTER IN POSSESSION OF THIS COURIER MAY BE SUBJECT TO PENALTY OF LAW.				
THIS CREDENTIAL IS THE PROPERTY OF THE UNITED STATES GOVERNMENT. ITS COUNTERFEITING, ALTERATION, OR MISUSE IS A VIOLATION OF SECTIONS 499 AND 701, TITLE 18, U.S. CODE.				
IF THIS CREDENTIAL IS FOUND, CALL COLLECT IMMEDIATELY, THE ALBUQUERQUE OPERATIONS OFFICE, 506-264-8952.				
EXPIRES _____				
DIRECTOR TSD, ALO-DOE, CERTIFYING OFFICIAL				

**EXAMPLE**

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

ORDER

DOE 5632.1

7-18-79

SUBJECT: PHYSICAL PROTECTION OF CLASSIFIED MATTER

---

1. PURPOSE. This Order prescribes the Department of Energy (DOE) policies and objectives as well as the responsibilities and authorities of Headquarters and field offices for the physical protection of classified matter.
2. CANCELLATION. Interim Management Directive (IMD) 6102, Serial No. 24, PHYSICAL PROTECTION FOR CLASSIFIED MATTER AND INFORMATION, of 6-29-77, as extended by DOE N 1321.45, of 6-26-79.
3. SCOPE. This Order applies to Departmental elements, including the Federal Energy Regulatory Commission (FERC), and to DOE contractors, subcontractors, and consultants who originate, receive, process, handle, store, transmit, dispose of, or are otherwise entrusted with the custody of, or access to, classified matter.
4. POLICY AND OBJECTIVES.
  - a. Classified matter shall, as a minimum, be subject to access controls and afforded physical protection in accordance with the standards and procedures specified in directives of the 5632 series.
  - b. Physical protection afforded classified matter should be optimized in terms of the most efficient, effective, and economical means available.
  - c. When it is impracticable to meet a specific standard or procedure, other means for providing an equivalent level of protection may be utilized, subject to approval by the Director of Safeguards and Security (DP-30) for Headquarters activities or by the head of the responsible field organization.
  - d. When special nuclear material (SNM) is classified because of its configuration or composition, or is contained within or is part of a classified item, it shall be afforded the higher of the levels of physical protection required by Physical Protection Standards for Classified Matter, 5632.2, Physical Protection of SNM, of 2-16-79, for the quantity Category of SNM involved or by other applicable directives.

---

DISTRIBUTION:  
All Departmental Elements  
Federal Energy Regulatory Commission

INITIATED BY:  
Office of Safeguards  
and Security



5. RESPONSIBILITIES AND AUTHORITIES.

## a. Assistant Secretary for Defense Programs (DP-1):

- (1) Approves and establishes policies, standards, and procedures for physical protection of classified matter.
- (2) Authorizes security shipments outside the United States, other than those consigned to nuclear explosive test sites, after DP-30 advises as to the adequacy of the security measures for such shipments.
- (3) Authorizes, through the Director of Military Application (DP-20), the transmission of classified matter which reveals or is identified as weapon data to the Department of Defense (DOD), its military components and contractors or subcontractors, and to foreign governments under agreements for cooperation.

b. Director of Safeguards and Security (DP-30):

- (1) Develops for approval by DP-1, policies, standards, and procedures for the physical protection of classified matter, in coordination with Headquarters divisions and offices and field offices.
- (2) Provides staff assistance on physical protection of classified matter to Secretarial Officers, DOE Staff Offices and to heads of field organizations.
- (3) Evaluates the adequacy of security measures for security shipments to destinations outside the United States, other than shipments to nuclear explosive test sites, and advises DP-1.
- (4) Procures and distributes to field offices inserts for DOE employee identification badges, and other credentials, excluding those issued to DOE couriers assigned to the Albuquerque Operations Office Transportation Safeguards Division (AL-TSD) and those issued by the Inspector General (IG-1) and the IG staff.
- (5) Disseminates reports of losses and recoveries of DOE employee identification badges, and other credentials, excluding those issued to DOE couriers assigned to the AL/TSD, and those issued by the IG-1 to the IG staff.

- (6) Conducts research and development in physical protection technology and equipment to meet safeguards and security requirements, and provides information about this technology to Secretarial Offices, DOE Staff Officers, and to heads of field organizations.
- (7) Reviews and comments on exceptions to the provisions of this Order and those of the 5632 series approved by heads of field organizations on the basis of site-specific considerations.
- (8) Report losses of classified matter.
- (9) With respect to Headquarters and Headquarters-administered contracts:
  - (a) Assures that classified matter is physically protected in accordance with standards contained in this Order and those of the 5632 series.
  - (b) Approves the holding of classified conferences outside of DOE security areas.
  - (c) Takes measures to detect surreptitious listening devices at security facilities and at classified conference locations outside of DOE security areas.
  - (d) Assembles, laminates, and issues DOE employee identification badges and other credentials, excluding those issued by IG-1 to the IG staff.
  - (e) Authorizes, pursuant to section 161k of the Atomic Energy Act of 1954, as amended, the carrying of firearms, as necessary, by DOE couriers and other DOE and DOE contractor and subcontractor personnel.
  - (f) Assures that lists of prohibited articles are posted conspicuously at entrances to security areas.
  - (g) Grants exceptions to the provisions of this Order.
  - (h) Approves and monitors the implementation of occasion-specific physical security plans for office space relocations which involve the movements of classified matter and security repositories.

c. Secretarial Officers, DOE Staff Officers and Chairman, Federal Energy Regulatory Commission:

- (1) Assure that classified matter in their organizations is physically protected in accordance with the requirements of this Order and those of the 5632 series.
- (2) Request approval from DP-30 for the holding of classified conferences outside of DOE security areas.
- (3) Provides coordination with the Office of Safeguards and Security in the development of security policies, standards, and procedures.
- (4) Prepare occasion-specific physical security plans for office space relocations which involve the movements of classified matter and security repositories and provide copies to DP-30 for approval and to the Director of Administrative Services (AD-40) for implementation.
- (5) Authorize employees under their jurisdiction to handcarry classified matter (excluding matter classified Top Secret) between security facilities within the United States. Until issued as a directive, procedures for transmission of Top Secret matter may be obtained from the Office of Classification, DP-60.
- (6) Approve the shipment of classified matter, other than nuclear explosives or other matter which reveals or is identified as weapon data, to the DOD and its military components, to other government agencies, and to their contractors, or subcontractors, and to foreign governments under agreements for cooperation.
- (7) Report losses of classified matter.

d. Director of Military Application (DP-20):

- (1) In addition to the responsibilities outlined in subparagraph 5c, directs the DOE Transportation Safeguards System for the domestic shipments of nuclear explosives; Category I quantities of SNM, excluding Naval Reactor (NR) core shipments; classified configurations or Category II quantities of SNM as requested by responsible outlay program managers; and any form of Pu-238 in excess of five grams. NR core shipment program responsibility rests with the Director, Division of Naval Reactors.

- (2) Develops and implements with the approval of DP-1, policies and procedures regarding the transmission of classified matter to the DOE, its military components, their contractors or sub-contractors and to foreign governments.
  - (3) Reviews and coordinates the development of safeguards technology to deter and protect against theft of nuclear explosives, their components, and SNM in transit.
- e. The Director of Administration (AD-1), through the Director of Administrative Services (AD-40): In addition to the responsibilities outlined in subparagraph 5c, implements approved occasion-specific physical security plans for office space relocations which involve the movements of classified matter and security repositories.
- f. Director of Administration (AD-1), through the Director of Construction and Facility Management (AD-30):
- (1) In addition to the responsibilities outlined in subparagraph 5c, develops general design criteria and construction standards to be applied in design and construction of DOE facilities.
  - (2) Incorporates, in these criteria and standards, the design and construction requirements for physical protection of classified matter, with input, advice, and guidance from DP-30 and from Headquarters outlay program managers to assure integration and compatibility with programmatic considerations.
  - (3) Provides engineering and construction support to program officials and field offices in construction project planning and execution.
- g. Heads of Field Organizations:
- (1) Assure that classified matter is physically protected in accordance with the requirements of this Order and those of the 5632 series.
  - (2) Approve the holding of classified conferences outside of the DOE security areas.
  - (3) Obtain:
    - (a) From the Manager, Nevada Operations Office, approval for the release of security shipments to nuclear explosive test sites outside the United States.

- (b) From DP-20, approval for the transmission of DOE classified matter revealing or identified as weapon data to the DOD, its military components and its contractors, or subcontractors.
- (4) Authorize DOE, and DOE contractor or subcontractor employees to hand-carry classified matter (excluding matter classified Top Secret) between security facilities within the United States.
  - (5) Request DP-30 to evaluate and advise DP-1 as to the adequacy of security measures for transporting security shipments outside the United States, other than those consigned to nuclear explosive test sites.
  - (6) Authorize, in accordance with section 161k of the Atomic Energy Act of 1954, as amended, the carrying of firearms by DOE couriers and other DOE and DOE contractor and subcontractor personnel as necessary.
  - (7) Coordinate security shipments with other field office heads for maximum economy.
  - (8) Approve, as deemed necessary, manuals and instructions prepared by contractors or subcontractors to implement the provisions of directives in the 5632 series.
  - (9) Take measures to detect surreptitious listening devices at security facilities and at classified conference locations.
  - (10) Advise DP-30 when site specific considerations dictate the use of equipment for which no DOE test data are available. The responsible field office shall insure that the selection of equipment to be used is made to the extent possible based on data provided in appropriate DOE safeguards handbooks. If site specific considerations dictate that the system include components for which no DOE test data are available, the assistance of DP-30 should be requested.
  - (11) Assemble, laminate, and issue DOE employee identification badges, and other credentials.
  - (12) Report losses and recoveries of DOE identification badges, and other credentials promptly to DP-30.
  - (13) Report losses of classified matter, in accordance with directives in the 5633 series.

- (14) Coordinate with DP-30 proposed changes in security arrangements or alterations in security areas or major facilities, national laboratories, and DOE offices which will bring about substantial changes in the degree of physical protection provided for classified matter.
  - (15) Approve the transmission of classified matter, other than that which reveals or is identified as weapon data, to the DOD and its military components, to other outside agencies, and to their contractors, or subcontractors.
  - (16) Report immediately to DP-30 any untoward incident involving the carrying, discharge, or other use of firearms or any incident involving use of aerosol irritants, tear gas, or other chemical agents by DOE authorized protective personnel.
  - (17) Assure that lists of prohibited articles are posted conspicuously at entrances to security areas.
  - (18) Grant exceptions to the requirements of this directive and notify DP-30 promptly in writing.
- h. Manager, Nevada Operations Office: In addition to the responsibilities outlined in subparagraph 5g, approves the release of security shipments between DOE and military installations within, and nuclear explosive test sites outside, the United States. The Commander of the Task Force assigned to conduct overseas nuclear explosive tests also has this authority.
- i. Managers, Albuquerque, Nevada, Oak Ridge, San Francisco, and Savannah River Operations Offices: In addition to the responsibilities outlined in subparagraphs 5g and 5h as applicable, approve the transmission of DOE classified matter revealing or identified as weapon data to the DOD, its military components and its contractors or subcontractors, or to foreign governments under agreements for cooperation, upon specific delegation of authority by DP-1 through DP-20.
- j. Manager, Albuquerque Operations Office (ALO):
- (1) In addition to the responsibilities outlined in subparagraphs 5g and 5i, manages the DOE Transportation Safeguards System for the domestic shipments of nuclear explosives; Category I quantities of SNM, excluding naval reactor (NR) core shipments; classified configurations of Category II quantities of material as requested by responsible outlay program managers; and any form of Pu-238 in excess of five grams. NR core shipment responsibility rests with the Pittsburgh Naval Reactors Office (PNR).

- (2) Conducts surveys of security shipments under ALO jurisdiction or requests another DOE organization to conduct such surveys.
  - (3) Submits reports of surveys made pursuant to (2), above, to DP-30 and the appropriate outlay program managers.
  - (4) Operates the nationwide secure communications (SECOM) system in support of the DOE Domestic Transportation Safeguards System.
6. PROCEDURES AND REQUIREMENTS. Specific standards, procedures and requirements for the protection of classified matter will be issued as soon as possible as directives in the 5632 series.

FOR THE SECRETARY OF ENERGY:



William S. Heffelfinger  
Director of Administration

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

ORDER

DOE 5632.2

2-16-79

SUBJECT: PHYSICAL PROTECTION OF SPECIAL NUCLEAR MATERIALS

1. PURPOSE. This Order establishes minimum physical protection standards for special nuclear materials (SNM). These and other security standards, when integrated with the material control and accountability standards in the Department of Energy (DOE) safeguards and security directives, provide the basis for a graded safeguards and security system for deterring, preventing, and effectively counteracting (through coordination and initiation of recovery and the minimization of consequences) theft of SNM by an adversary with or without inside collaboration. (See separate classified guidance on credible threat characterization provided by the Office of Safeguards and Security.)
2. CANCELLATION AND SPECIAL INSTRUCTIONS. Interim Management Directive 6103, PHYSICAL PROTECTION OF SPECIAL NUCLEAR MATERIAL, of 9-29-77, as extended by DOE N 1321.25 of 11-27-78. The access authorization requirements of subparagraphs 8f(2), 8g(1)(a)1, 8g(1)(b)1, and 8g(1)(c) of this Order shall be held in abeyance pending publication in the Federal Register of appropriate revisions to 10 CFR Part 710 to legally establish those requirements.
3. SCOPE. The provisions of this Order apply to all elements of the Department of Energy and to contractors and subcontractors to the extent they possess SNM not subject to a Nuclear Regulatory Commission (NRC) license.
4. SPECIAL CONDITIONS. The provisions of this Order, or the level of protection applied to SNM, may be reduced when one or more of the following conditions exist:
  - a. The SNM is not readily separable from other radioactive material and the combination of the SNM and other radioactive material delivers an external radiation dose of approximately 100 rems per hour or more at 1 meter from any accessible surface without intervening shielding material.
  - b. The SNM is contained in material that has been declared as waste.
  - c. The SNM is in a chemical, isotopic, or physical form or is within isolated in-process, or remote inaccessible, containment which provides comparably effective protection, to that specified herein, against malevolent use or theft.

DISTRIBUTION:  
All Departmental Elements  
Federal Energy Regulatory Commission (info)

INITIATED BY:  
Office of Safeguards  
and Security

GPO 925-697

3



- d. Where the foregoing conditions exist, they should be specifically and clearly described in the facility safeguards and security plan to demonstrate a logical basis for the physical protection system provided. When material is to be shipped, it shall be the responsibility of the shipper to determine if any of these conditions exist. At certain facilities, a level of physical protection exceeding that specified herein may be necessary in order to assure a satisfactory level of integrated safeguards and security system effectiveness.
5. POLICY AND OBJECTIVES. It is DOE policy to physically protect all SNM against theft. This Order is designed to facilitate effective safeguards and security systems through graded and performance-evaluated physical protection requirements for SNM. The minimum standards have been so designed as to satisfy the policy requirement that the effectiveness of nuclear safeguards and security systems in DOE activities provide comparable effectiveness with that required of licensees by the Nuclear Regulatory Commission.
6. DEFINITIONS.
  - a. Albuquerque Operations Office, Transportation Safeguards Division (ALO/TSD) Courier. A "Q" cleared employee of the Transportation Safeguards Division, Albuquerque Operations Office, who is authorized under Section 161.k. of the Atomic Energy Act of 1954, as amended, or other appropriate statutory authority, to carry firearms, and who is employed and charged with the responsibility for the safe secure movement of nuclear explosives, classified nuclear components, and Category I quantities of SNM in the DOE Transportation Safeguards System.
  - b. Assessment. An onsite examination by the Headquarters Office of Safeguards and Security of the factors comprising the safeguards and security program administered by a DOE operations office and implemented by a DOE contractor. The purpose of the assessment is to determine the effectiveness of the operations office in assuring that DOE contractors are complying with the requirements of this and related safeguards and security directives and in administering an effective overall safeguards and security program.
  - c. Category "I" Quantities of SNM.
    - (1) Uranium 235 (contained in Uranium enriched to 20% or more in the isotope U-235) alone, or in combination with Plutonium and/or Uranium 233 when (multiplying the Plutonium and/or Uranium 233 content by 2.5) the total is 5,000 grams or more.

- (2) Plutonium and/or Uranium 233 when the Plutonium and/or Uranium 233 content is 2,000 grams or more.
- (3) SNM in lesser quantities but which is located in the same area or shipment with other SNM with which it could be selectively combined to produce the equivalent quantities in item (1) of this category.

d. Category II Quantities of SNM.

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

e. Category III Quantities of SNM have been further divided into two subcategories IIIA and IIIB:

(1) Category IIIA Quantities of SNM.

- (a) Uranium 235 (contained in Uranium enriched to 20% or more in the isotope U-235) when the total is 350 grams to 999 grams.
- (b) Plutonium and/or Uranium 233 when the Plutonium and/or Uranium 233 content is 220 grams to 399 grams.
- (c) Combinations of Plutonium and/or Uranium 233 with Uranium 235 (contained in Uranium enriched to 20% or more in the isotope U-235) when the total is less than 1,000 grams and the Plutonium and/or Uranium 233 content is less than 400 grams.

(2) Category IIIB Quantities of SNM.

- (a) Uranium 235 (contained in Uranium enriched to 20% or more in the isotope U-235) when the total of the U-235 content is 1 gram to 349 grams.

2-16-79

- (b) Plutonium and/or Uranium-233 when the Plutonium and/or Uranium 233 content is from 1 gram to 219 grams.
- (c) Uranium 235 contained in Uranium enriched to less than 20% in the isotope U-235 in all quantities above .99 grams.
- f. Courier. An armed DOE employee, or member of the Armed Forces assigned to and performing duties under the direction and control of the DOE, who possesses a "Q" access authorization or an equivalent Department of Defense (DOD) security clearance, and who is specifically charged with the armed protection of designated matter in transit.
- g. DOE-Approved Equipment. Equipment (i.e. alarm, assessment, monitoring, detection) used in conjunction with all other elements of the site safeguards and security system as described in the site specific safeguards and security plan (after such plan is approved by the responsible operations office).
- h. DOE Transportation Safeguards System. The DOE program, managed and operated by the Manager of the Albuquerque Operations Office (AL) under the programmatic direction of the Director of Military Application (DP-20), which has the administrative and courier personnel, special transport and escort vehicles, and nationwide HF communications system (SECOM) required to carry out the total responsibility for the safe secure domestic transportation of all DOE-owned or -controlled nuclear explosives and Category I quantities of SNM.
- i. Duress System. A system which can covertly communicate a situation of duress to a security control center or other safeguards and security personnel who can notify a security control center.
- j. Escort. A DOE or DOE contractor or common carrier employee specifically assigned for the delivery of a security shipment. Escorts include guards, truck drivers, and other attendants furnished by DOE, DOE contractors, or common carriers.
- k. Guard. See DOE 5632.1, "Physical Protection of Classified Matter and Information". (To be issued)
- l. Hardened Security Post. See DOE 5632.1.
- m. Intrusion Alarm System (perimeter or interior). Detection hardware and/or software comprised of (1) sensors, (2) alarm assessment systems, and (3) alarm reporting systems (including alarm communications and information display equipment).

- n. Material Access Area (MAA). An area containing a Category I quantity of SNM specifically defined by physical barriers, located within a protected area, and subject to specific access controls.
- o. Material Surveillance Procedures. Procedures to assure the observation of an area containing SNM by at least two cleared and authorized persons who may be doing other work but who can give an alarm in time to prevent the unauthorized removal of the SNM. One of the persons who maintains such surveillance must be "Q" cleared and the other must possess at least an "S" or "L" access authorization.
- p. Outlay Program Managers. The Assistant Secretaries for Conservation and Solar Applications, Resource Applications, Energy Technology, Environment, and Defense Programs, and the Director of Energy Research.
- q. Physical Barriers. See DOE 5632.1.
- r. Protected Area (PA). A specifically defined area enclosed by physical barriers meeting the standards contained in DOE 5632.1.
- s. Random Patrol. A patrol conducted in a manner such that the location of the patrol at any specific time cannot be predicted.
- t. Safeguards and Security Plan. A specific description of the systems and procedures implemented to protect special nuclear material.
- u. SECOM. The high frequency radio communications network operated by AL in support of transportation safeguards.
- v. Security Container.
  - (1) A metal security container approved by the General Services Administration for the storage of classified matter and marked "General Services Administration Approved Security Container." This container meets the Class 1 standards of Federal Specification AA-F-357, the Class 5 standards of Federal Specification AA-F-358, or the Class 5 standards of Federal Specification AA-F-363.
  - (2) A burglar-resistant cabinet or chest having a body of steel at least 1/2" thick, and a combination locked steel door at least 1" thick exclusive of bolt work and locking devices.
- w. Security Inspector. See DOE 5632.1.

- x. Security Room. One having combination-locked door(s) and protected by a DOE-approved intrusion alarm system actuated by any penetration of walls, floor, ceiling or openings, or by motion within the room.
- y. Special Nuclear Material (SNM). Means (1) plutonium, uranium enriched in the isotope 233 or in the isotope 235, and any other material which, pursuant to the provisions of Section 51 of the Atomic Energy Act of 1954, as amended, has been determined to be special nuclear material, but does not include source material; or (2) any material artificially enriched by any of the foregoing, but does not include source material.
- z. SNM Facility. An educational institution, a plant, laboratory, office, or building utilized by DOE, its contractors, subcontractors, or consultants and which contains SNM.
- aa. SNM Facility Approval. A determination based upon review of a safeguards and security plan and an onsite survey by the responsible DOE operations office that a facility is approved to receive, use, process, and/or store SNM.
- bb. SNM Vault. A penetration-resistant, windowless enclosure which:
  - (1) Has walls, floor, and ceiling substantially constructed of materials which afford a forced penetration resistance at least equivalent to that of 8 inch thick reinforced concrete; (2) has 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; (3) has a built-in combination locked steel door which in existing structures is at least 1" thick exclusive of bolt work and locking devices and which for new structures at least meets the class 5 standards of Federal Specification AA-D-600B; and which (4) can constitute one of the barrier elements of a site-specific integrated safeguards and security physical protection system and which, in conjunction with other measures, will prevent successful completion of an attempted forcible theft of SNM.
- cc. Survey. An on-the-spot critical examination by the responsible DOE operations office of an SNM facility or SNM shipment and devices, equipment, and procedures employed to protect the SNM involved.
- dd. Waste. A term applied to any source and special nuclear material which is no longer useful. Includes that which has become radioactive by any means to the extent that the material itself exhibits an emission of radioactivity of such a level that it must be handled and disposed of by special methods in order to protect the general public. Also includes scrap which has been evaluated and determined to be uneconomical to recover, and which is not necessarily radioactive.

7. RESPONSIBILITIES AND AUTHORITIES.

a. Director of Safeguards and Security (Assistant Secretary for Defense Programs).

- (1) Develops and establishes policies and ensures that requirements, standards, and criteria for the physical protection of SNM are developed in coordination with appropriate Headquarters organizations and operations offices.
- (2) Provides advice and technical assistance on the physical protection of SNM to outlay program managers and to managers of operations offices.
- (3) Reports immediately to the Under Secretary, Assistant Secretary for Defense Programs, Inspector General, concerned outlay program managers, and the Federal Bureau of Investigation any information related to actual or attempted theft of SNM or any circumstances indicating a violation of Federal law concerning such material.
- (4) Conducts assessments, and informs the appropriate operations office manager and outlay program manager of the results in a timely manner, and coordinates with appropriate DOE organizations to correct deficiencies, including those which have a program or budgetary impact.
- (5) Provides assistance to appropriate outlay program managers and operations office managers in development of the safeguards and security plan for each DOE SNM facility.
- (6) Reviews and comments on safeguards and security plans for site specific application.
- (7) Conducts research and development in physical protection technology and equipment to meet safeguards and security requirements, and provides information about this technology to the nuclear community both domestically and internationally.
- (8) Assures comparable effectiveness of DOE safeguards and security systems with those required by the Nuclear Regulatory Commission.
- (9) Reviews and comments on exceptions to the provisions of this directive approved by managers of operations offices on the basis of site specific applications.

b. Assistant Secretary for Environment.

- (1) Advises and recommends DOE policy and standards as relates to personnel and environmental protection from radioactive materials

and overview and appraisal of all operations to assure compliance with such policy and standards.

- (2) Participates in the development of procedures and methods for implementing DOE policies and standards for the safe transportation of SNM.
- (3) Serves as the primary point of contact with the transportation industry and Federal, State, and local agencies in implementing DOE's transportation policies and standards.

c. Outlay Program Managers.

- (1) Report immediately to the DOE Emergency Operations Center any information related to an actual, attempted, or suspected theft of SNM or any other circumstances indicating a violation of Federal law concerning such material.
- (2) Require the preparation of safeguards and security plans for facilities and programs for which they have programmatic responsibility and assist in the development of such plans in coordination with the Director of Safeguards and Security.
- (3) Develop and support programs and budgets necessary to assure that special nuclear materials under their programmatic jurisdiction are protected in accordance with this Order in coordination with operations offices, and the Office of Safeguards and Security.
- (4) Consult with the Director of Safeguards and Security on questions concerning safeguards and security requirements and other matters pertaining to the physical protection of SNM.
- (5) Provide, in coordination with the Office of Safeguards and Security, appropriate guidance to responsible operations offices on actions to be taken with respect to implementing safeguards and security systems and procedures.
- (6) Perform reviews, as necessary, to evaluate safeguards and security program funding of activities involving SNM under their programmatic jurisdiction.

d. Director of Military Application (DP-20).

- (1) Directs the DOE Transportation Safeguards System for the domestic shipments of nuclear explosives; Category I quantities of SNM, excluding naval reactor (NR) core shipments; classified configurations of Category II quantities of SNM as requested by responsible outlay program managers; and any form of Pu-238 in excess of five grams. (NR core shipment program responsibility rests with the Director, Division of Naval Reactors).

Table I  
PHYSICAL PROTECTION  
CATEGORIZATION OF NUCLEAR MATERIAL

Special Nuclear Material	Category I*	Category II*	Category III-A**	Category III-B
Plutonium	2 kgs. or more	400-1,999 grams	220-399 grams	1-219 grams
U-233	2 kgs. or more	400-1,999 grams	220-399 grams	1-219 grams
Uranium-235 Contained in Uranium enriched to 20% or more.	5 kgs. or more	1,000-4,999 grams	350-999 grams	1-349 grams
Uranium-235 (Contained in Uranium enriched to less than 20%).	-	-	-	All quantities above .99 grams

\* If Plutonium or U-233 is combined with U-235, the amounts of Pu or U-233 shall be multiplied by 2.5 to arrive at the limits shown.

\*\* A plutonium and/or Uranium 233 content of less than 400 grams may be combined with Uranium 235 when the total content is less than 1000 grams.



- (6) Report immediately to the DOE Emergency Operations Center and to the FBI any information related to an actual, attempted, or suspected theft of SNM or any other circumstance indicating a violation of Federal law concerning such material.
- (7) Evaluate and report to the Director of Safeguards and Security and to the cognizant outlay program manager any actual or attempted theft of SNM.
- (8) Perform planning for funding and staffing to implement this directive.
- (9) Conduct surveys and submit reports pertaining to SNM facilities and shipments to the Director of Safeguards and Security and to the responsible Headquarters outlay program manager.
- (10) Establish and document, as appropriate, the support to be expected from local law enforcement agencies.
- (11) Require overt testing of the physical protection system to verify the maintainance of a continuing high state of effectiveness against attack.
- (12) Report annually by, December 1, to the Under Secretary, with copies to the Assistant Secretary for Defense Programs, the Inspector General, outlay program managers, and the Director of Safeguards and Security, on the state of safeguards and security of SNM under their responsibility.

g. Manager, Albuquerque Operations Office (AL).

- (1) In addition to the responsibilities outlined in subparagraph 7f manages the DOE Transportation Safeguards System for the domestic shipments of nuclear explosives; Category I quantities of SNM, excluding naval reactor (NR) core shipments; classified configurations of Category II quantities of material as requested by responsible outlay program managers; and any form of Pu-238 in excess of five grams. (NR core shipment responsibility rests with the Pittsburg Naval Reactors Office [PNR]).
- (2) Conducts surveys of SNM shipments under his jurisdiction or requests another DOE organization to conduct such surveys.
- (3) Submits reports of surveys made pursuant to subparagraph 7g(2) to the Director of Safeguards and Security and to the responsible Headquarters outlay program manager.
- (4) Operates the nationwide SECUM system in support of the DOE Domestic Transportation Safeguards System.

- (2) Reviews and coordinates the development of safeguards technology to deter and protect against theft of nuclear explosives, their components and SNM in transit.

e. Director of Administration, through the Director of Construction and Facility Management.

- (1) Develops general design criteria and construction standards to be applied in design and construction of DOE facilities.
- (2) Incorporates, in these criteria and standards, the design and construction requirements for physical protection of SNM, with input, advice, and guidance from the Office of Safeguards and Security.
- (3) Provides engineering and construction support to program officials and operations offices in construction project planning and execution.

f. Managers of Operations Offices.

- (1) Assure that SNM is afforded physical protection in accordance with this directive.
- (2) Require, review, and approve written site-specific safeguards and security plans, in consultation with appropriate Headquarters outlay program managers, and submit plans and major changes thereto to the Director of Safeguards and Security for review and comment.
- (3) Grant exceptions to the requirements of this directive and notify the Director of Safeguards and Security, promptly in writing, with a copy to the cognizant outlay program manager.
- (4) Notify the Director of Safeguards and Security of the establishment of SNM facilities.
- (5) Advise the Director of Safeguards and Security when site specific considerations dictate the use of equipment for which no DOE test data are available. The responsible operations office shall insure that the selection of equipment to be used is made to the extent possible based on data provided in appropriate DOE safeguards handbooks. If site specific considerations dictate that the system include components for which no DOE test data is available, the assistance of the Office of Safeguards and Security should be requested.

- (6) Security inspector posts, both mobile and fixed, shall be equipped with duress systems.
- (7) Government-owned or Government-leased vehicles shall be admitted only when on official business and when operated by properly cleared and authorized drivers or who are under escort by properly cleared and authorized personnel.
- (8) Service and delivery vehicles shall be admitted to protected areas only when on authorized business and when driven or under escort by properly cleared and authorized personnel. Access by such vehicles shall be kept to a minimum consistent with operational requirements.
- (9) Personnel, packages, briefcases and similar containers, and all vehicles shall be subject to search at the entrance to a protected area. The search on entering, when performed, may be made with DOE-approved detection equipment designed to assure that explosives, weapons, or other prohibited articles are not introduced. (ALO/TSD personnel and equipment shall be exempt from this requirement when on official business).
- (10) A search of personnel, packages, briefcases and similar containers, and all vehicles shall be made prior to leaving a material access area or protected area to assure that SNM is not being surreptitiously removed. The search may be carried out by using DOE-approved detection equipment. Detection equipment may be installed at material access areas, or at protected area exits if special control measures have been implemented to close unguarded diversion paths.
- (11) Signs prohibiting trespassing shall be posted on the protected area fences. Appropriate reward signs, and signs prohibiting the introduction of contraband articles and authorizing the searches of personnel, packages, briefcases and similar containers, and vehicles either entering or exiting shall be posted at entrances to protected areas and material access areas.
- (12) Perimeter intrusion alarm systems or equivalent means of providing early detection shall be used at the perimeters of protected areas or material access areas.

8. PROCEDURES AND REQUIREMENTS.

a. General.

- (1) A facility shall not receive, use, process, or store SNM until an SNM facility approval, based upon a review of the safeguards and security plan and an on-site survey by the responsible operations office, has been granted.
- (2) Continual vigilance shall be maintained for procedural violations or practices inconsistent with physical protection measures afforded SNM.
- (3) Any unauthorized attempts, suspected attempts, or actual removals of special nuclear material from a protected area or material access area shall be reported immediately to the responsible DOE Safeguards and Security office.
- (4) Reports, plans, and data relating to the protection and control of SNM shall be classified in accordance with Classification Guide CG-S-1, and other applicable classification guides.

b. Specific Requirements for Protected Areas.

- (1) Protected areas shall be subject to a system of access controls administered by security inspectors who meet the standards contained in DOE 5632.1.
- (2) A sufficient level of illumination shall be provided at all points on the perimeter to permit assessment in the event of unauthorized attempts to penetrate the protected area.
- (3) A hardened security force communications center shall be established and shall have periodically tested radio and telephone channels of communication with local law enforcement agencies. There also shall be an emergency alternate communications capability from a secondary station for use in event the primary station is compromised.
- (4) Radio communications equipment used in subparagraph 8b(?) shall remain operable in the event of a loss of primary electrical power.
- (5) Private use vehicles shall be excluded.

intrusion alarm systems; with a security inspector response time of not more than 5 minutes.

- (3) SNM shall be in storage or under material surveillance procedures, or protected in accordance with subparagraph 8c(1), above.
  - (4) A hardened security post shall be established where the protection of the security inspector is vital to the reporting of unauthorized penetration of the area perimeter alarms. This may be located within or on the perimeter of the protected area.
  - (5) Records shall be maintained of all persons who are admitted to material access areas who are not directly employed in operations involving access to, use, processing, storage, accountability, or protection of SNM and of all persons who enter such areas during nonoperating hours.
- d. Protection of Category I Quantities of SNM - In Use or Storage.
- (1) Category I quantities of SNM shall be used, processed, or stored only within material access areas enclosed within a protected area.
  - (2) Any person in a position to divert or to conceal the diversion of Category I quantities of SNM shall possess a DOE "Q" security clearance. Uncleared persons may be permitted access to a protected area only under escort of an "S," "L," "TS," or "Q" cleared individual and to a material access area only under escort of a "Q" cleared person. (Note: Equivalent clearances may be used subject to individual determination.)
  - (3) SNM facilities holding Category I quantities of SNM shall be surveyed to evaluate the adequacy of physical protection provisions at least annually. In addition, surveys should be conducted as often as is necessary to maintain a high standard of performance as determined by the responsible operations office manager. Reports of surveys shall be furnished promptly to the Director of Safeguards and Security and to the responsible outlay program manager.
- e. Protection of Category I Quantities of SNM and Classified Configurations of Category II Quantities of SNM - In Transit.
- (1) Shipments of Category I Quantities of SNM and classified

- (a) As an alternative, until a protected area or material access area can be placed under perimeter alarm protection (or its equivalent), it shall be occupied by at least two security inspectors who shall have immediately available one or more DOE-approved night vision devices, and at least two means of communication (i.e., telephone and radio) to a point from which response forces can be dispatched.
  - (b) During times when the perimeter alarm or equivalent is not in operation, the perimeter shall be patrolled (on a random basis) by security inspectors at intervals not exceeding 1 hour.
- (13) All detection/alarm devices, including transmission lines to annunciators shall be failure, and tamper-indicating. Such devices shall be connected to monitor/display panels in the hardened security force communications center required in subparagraph 8b(3). An alternate alarm annunciation point (or a comparable alternate capability) shall be provided in a location which is continuously manned by cleared personnel and which provides a second indication of an alarm such that a response can be initiated in the event the primary station is compromised.
- (14) All security related subsystems and components shall be maintained in readily operable condition, and shall have a test and maintenance program to assure an effective operable condition.

c. Specific Requirements for Material Access Areas.

- (1) Unoccupied rooms or buildings (or a portion of a building) within a material access area containing Category I quantities of in-process SNM shall be equipped with DOE-approved intrusion alarm systems, or other equally effective means. Protection of Category II and Category III quantities of SNM located within a material access area should be in accordance with the requirements of 8f or 8h, respectively. Security Inspector response time to alarms shall be not more than 5 minutes. Access to such rooms shall be controlled to limit entry to appropriately cleared or escorted individuals who require admittance to perform their official duties.
- (2) Category I quantities of SNM shall be stored in SNM vaults; or in a security room which is equipped with DOE-approved

- (b) Train. Nonweapons parts weighing less than 5,000 pounds, but more than 1,000 pounds per unit must be shipped in locked and sealed rail cars accompanied by at least three DOE couriers. Individual units (excluding nuclear weapons or devices) weighing over 5,000 pounds can be shipped on flatcars accompanied by only one courier. Couriers accompanying train shipments shall utilize SECOM communications.
- (c) Air Transportation. If not otherwise prohibited by statute or implementing instructions, air shipments may take place in aircraft owned by DOE or under DOE contract, with the material in the custody of at least two ALU/TSD couriers with pilot(s) and other crew members possessing "Q" access authorization. The cargo when in their custody, shall be under the direct observation of the couriers during all land movements and loading and unloading operations.
- (2) There shall be a detailed search of the transport vehicle prior to loading and shipment to ensure that sabotage devices (that could facilitate theft of the SNM) have not been implanted or that sabotage has not been initiated, and that unauthorized persons are not aboard.
- (3) Written procedures approved by the responsible operations office shall be followed by courier personnel responsible for the shipment of SNM.
- (4) Courier Receipt, Form DOE-60, or equivalent shall be executed at all points where the SNM in-transit changes custody.
- (5) Shipments shall be scheduled in irregular patterns and pre-planned to avoid areas or routes having high risk and areas of natural disaster or civil disorders, such as strikes or riots.
- (6) Couriers shall maintain continued vigilance for the presence of conditions or situations which might threaten the security of the shipment, take such action as circumstances might require to avoid interference with continuous safe secure passage of the cargo vehicle, provide assistance to or summon aid for the crew of the cargo vehicle in case of emergency, check seals or locks at each stop where time permits, and observe the cargo vehicle and adjacent areas during stops or layovers.

configurations of Category II quantities of SNM shall be made by one of the following methods:

(a) Highway.

- 1 In locked and sealed safe secure trailers (SST), towed by special tractors, accompanied by at least six ALU/TSD couriers. All convoy vehicles will be driven by ALU/TSD couriers.
- 2 Tractors and escort vehicles shall maintain intra convoy communication with VHF radios and two-way communication with the SECUM Control Center with HF (SECUM) radios.
- 3 The vehicle containing the shipment shall be continuously guarded during the trip.
- 4 All shipments shall be made without intermediate stops, except for emergency reasons, driver relief, meals, refueling, or to transfer cargo.
- 5 At least one escort vehicle will accompany each shipment.
- 6 Shipments of individual units containing Category "I" quantities of SNM which weigh over 5,000 lbs. may be transported using conventional or flatbed trailers in accordance with a special plan approved by the Manager of AL (or Manager of PNR for NR core shipments) after coordination with the Office of Safeguards and Security.
- 7 Movements of Category "I" quantities of SNM between protected areas in the same site or between protected areas and loading areas at the same site, shall be escorted by couriers or security inspectors in a two-way radio-equipped vehicle. Such movements may be made by SST or security approved conventional vehicles.
- 8 Movements of Category "I" quantities of SNM within a protected area shall be under material surveillance procedures.



for Defense Programs or appropriate designees. Significant violations of procedures by couriers shall be reported immediately to the Manager of AL, and after evaluation to the Director of Safeguards and Security.

f. Protection of Category II Quantities\* of SNM - In Use or Storage.

- (1) Category II quantities of SNM shall be used, processed, and stored in a protected area. The protected area requirements specified in subparagraph 8b may be reduced subject to detailed justification contained in the approved site-specific safeguards and security plan.
- (2)\*\*Any person in a position which will permit him to divert or to conceal the diversion of Category "II" quantities of SNM shall possess a DOE "Q" security clearance. Uncleared persons may be permitted access to a protected area only under escort of an "S," "L," "TS," or "Q" cleared individual. (Note: Equivalent clearances may be used subject to individual determination.)
- (3) SNM facilities holding Category II quantities of SNM shall be surveyed to evaluate the adequacy of physical protection provisions at least annually. In addition, surveys should be conducted as often as is necessary to maintain a high standard of performance as determined by the responsible operations office manager. Reports of surveys shall be furnished to the Director of Safeguards and Security and to the responsible outlay program manager on a timely basis.
- (4) Unoccupied rooms or buildings (or a portion of a building) containing Category II quantities of in-process SNM shall be equipped with DOE-approved intrusion alarm systems, or other equally effective means. Access to such rooms shall be controlled to limit entry to individuals who require admittance to perform their official duties. Security inspector response time to alarms shall not be more than 10 minutes.

---

\* See Attachment I and Definitions, paragraph 6.

\*\* The access authorization requirements of this paragraph shall be held in abeyance pending publication in the Federal Register of appropriate revisions to 10 CFR Part 710.

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

2-16-79

(b) Train.

1\*\*Category II quantities of SNM may be shipped by train in the custody of at least two escorts possessing "L" access authorizations.

2 Cargo compartments shall be locked and sealed.

3 Escorts shall maintain frequent periodic communication with a control station which can request appropriate law enforcement agency response.

4 Escorts shall maintain the shipment under surveillance during the trip.

5 There should be a detailed search of the transport vehicle prior to loading and shipment to ensure that sabotage has not been initiated and that unauthorized persons are not aboard.

(c) \*\*Air Transportation. If not otherwise prohibited by statute or implementing instructions, air shipments of Category "II" quantities of SNM may take place. The material must be attended by at least two escorts possessing "L" access authorization or equivalent. The shipments must be under the direct observation of the escorts during all land movements and loading and unloading operations.

- (2) Procedures approved by the responsible operations office manager shall be followed by all personnel associated with the shipment.
- (3) Form DOE-60, or equivalent, shall be executed at all points where the in-transit SNM changes custody.
- (4) Route choice and schedule should be based on consideration to avoid areas of natural disasters or civil disorders and to provide the minimum number of cargo transfers and minimum length of transit time.
- (5) Movements of Category II quantities of SNM within a protected area shall be under material surveillance procedures.

---

\*\*

The access authorization requirements of this paragraph shall be held in abeyance pending publication in the Federal Register of appropriate revisions to 10 CFR Part 710.

- (5) Category II quantities of SNM shall be stored in vaults, security rooms, or security containers which are protected with DOE-approved intrusion alarm systems, with a security inspector response time of not more than 10 minutes.
  - (6) The SNM shall be in storage or under material surveillance procedures, or meet the conditions of subparagraph 8f(4).
- g. Protection of Category II Quantities of SNM - In Transit. (See subparagraph 8e for in transit protection for classified configurations of Category II quantities of SNM.)
- (1) Shipments of Category II quantities of SNM shall be made by one of the following methods:
    - (a) Truck.
      - 1\*\*Category II quantities of SNM may be shipped by government-owned or exclusive-use truck by commercial carrier in the custody of at least two escorts possessing "L" access authorizations or equivalent.
      - 2 Cargo compartments of the trucks shall be locked and sealed.
      - 3 Escorts shall maintain frequent periodic communication with a control station which can request appropriate law enforcement agency response.
      - 4 Escorts shall maintain the shipment under surveillance during the trip.
      - 5 All shipments shall be made without any intermediate stops (except for emergency reasons, and for driver relief, meals, refueling, or to transfer cargo in mixed modes of transportation, e.g., truck-to-train, etc.).
      - 6 There should be a detailed search of the transport vehicle prior to loading and shipment to ensure that sabotage devices have not been implanted or that sabotage has not been initiated and that unauthorized persons are not aboard.

\*\*\*

The access authorization requirements of this paragraph shall be held in abeyance pending publication in the Federal Register of appropriate revisions to 10 CFR Part 710.

- (c) Access to the material shall be limited to employees in positions which have been specifically designated by management as requiring access to Category IIIA quantities of SNM in the course of assigned duties and to authorized visitors who are under continuous escort of employees in such designated positions.
  - (d) Guard response to alarms shall be not more than 10 minutes.
  - (e) Packages, briefcases and similar containers, and all vehicles shall be subject to search by the individual controlling access to the use or storage area or to the protected area, if applicable. The search on entering shall be made to assure that explosives or other contraband are not introduced. Personnel and packages shall be subject to search upon leaving the use and storage area to assure that SNM is not being surreptitiously removed.
  - (f) Reward signs and signs prohibiting trespassing and the introduction of contraband articles and authorizing the searches of vehicles, packages, or persons either entering or exiting shall be posted at entrances to the use or storage area.
  - (g) SNM facilities holding Category IIIA quantities of SNM shall be surveyed to evaluate the adequacy of safeguards and security provisions at least every 2 years. Reports of inspections shall be furnished to the Director of Safeguards and Security and appropriate outlay program managers. In addition, surveys should be conducted as often as are necessary to maintain a high standard of performance.
- (2) Category IIIB\* quantities of SNM shall be received, used, processed, and stored in accordance with operations office approved safeguards and security plans.
- i. Protection of Category III Quantities of SNM - In Transit.
- (1) Shipments of all Category III quantities of SNM\*\* may be made by one of the following methods: truck, rail, air, or water in commercial for-hire vehicles.
  - (2) Packages shall be sealed.

\* See Attachment 1 and Definitions, paragraph 6.

\*\* If not otherwise prohibited by statute or implementing instructions, air shipments of Category "III" quantities of SNM may take place.

- (6) Movements of Category II quantities of SNM between protected areas at the same site shall be under escort by at least one security inspector.
- (7) Escorts shall maintain continued vigilance for the presence of conditions or situations which might threaten the security of the shipment, take appropriate action to avoid interference with continuous safe passage of the cargo vehicle, provide assistance to or summon aid for the crew of the cargo vehicle in case of emergency, check seals or locks at each stop where time permits, and observe the cargo vehicle and adjacent areas during stops or layovers.
- (8) In an emergency, where SNM is transferred from one vehicle to another, at least two cleared escorts shall keep the shipment under surveillance by observing all phases of the transfer, assuring that all the material is included in the second vehicle, and checking locks and seals.
- (9) Significant violations of procedures shall be reported immediately to the responsible operations office which shall, after making an evaluation, forward a written report to the Director of Safeguards and Security.
- (10) Safeguards and Security field organizations shall conduct necessary transportation security surveys of carriers at least annually. Surveys will be coordinated with the cognizant field transportation office.

h. Protection of Category III Quantities of SNM - In Use or Storage.

(1) Category IIIA\* Quantities of SNM.

- (a) When unattended, Category IIIA quantities of SNM shall be secured within a locked DOE-approved security container or within a locked room.
- (b) During nonworking hours the container or locked room containing the material shall be under protection of a DOE approved intrusion detection alarm system, or patrolled at intervals not to exceed 2 hours, or located in a protected area.

★

See Attachment 1 and Definitions, paragraph 6.

- (3) Shipments, excepting shipments of laboratory analysis samples, shall be made under arrangements which provide the capability to trace and identify, within 24 hours of request, the precise leg of a journey where a shipment went astray in the event of its nonarrival at destination within the prescribed time frame.
- (4) Advance notification of the estimated time of arrival to be received prior to dispatch, with written confirmation following not later than 48 hours after dispatch shall be provided by the shipper to the consignee.
- (5) The consignee will promptly notify the shipper by telephone upon determination that a shipment has not arrived within a reasonable time and shall provide written confirmation of such notification.
- (6) In the event that an exclusive use vehicle is required for other than safeguards and security reasons, the following provisions apply:
  - (a) The vehicle shall be given a detailed search prior to loading and shipment to ensure that sabotage devices have not been implanted or that sabotage has not been initiated.
  - (b) The vehicle shall be sealed and all seal numbers noted on the shipping papers.
- (7) Shipments shall be made in accordance with all applicable Federal regulations.

FOR THE SECRETARY OF ENERGY:



William S. Heffelfinger  
Director of Administration

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

ORDER

DOE 5632.3

11-18-81

SUBJECT: OPERATIONS SECURITY

- 
1. PURPOSE. To establish the Department of Energy (DOE) operations security program.
  2. SCOPE. The provisions of this Order apply to all classified and/or unclassified national security programs and is directed to all elements of the Department of Energy, including the Federal Energy Regulatory Commission (RC) and to contractors and subcontractors to the extent provided in the contract.
  3. REFERENCES.
    - a. DOE 5300.2, TELECOMMUNICATIONS: EMISSION SECURITY (TEMPEST), of 4-28-80, which establishes the Department of Energy telecommunications TEMPEST program for emission security and implements the provisions of the national policy which are applicable to emission security.
    - b. DOE 5631.2, PERSONNEL SECURITY PROGRAM, of 11-13-80, which implements the provisions of the Atomic Energy Act of 1954, as amended, and Executive Orders 10450, 10865, and 12065.
    - c. DOE 5632.1, PHYSICAL PROTECTION OF CLASSIFIED MATTER, of 7-18-79, which prescribes the Department of Energy policies and objectives as well as the responsibilities and authorities of Headquarters and field offices for the physical protection of classified matter.
    - d. DOE 5636.1, PROHIBITIONS ON WIRETAPPING AND EAVESDROPPING, of 7-11-78, which specifies the Department of Energy policy of prohibiting the procurement of devices designed specifically for wiretapping or eavesdropping and the installation or use of such equipment.
    - e. DOE 5300.1, TELECOMMUNICATIONS, of 12-19-78, which establishes policy and general guidance for the use, review, coordination, and provision of telecommunications services for the Department of Energy Headquarters and field organizations.
    - f. DOE 5636.2, SECURITY REQUIREMENTS FOR CLASSIFIED AUTOMATIC DATA PROCESSING SYSTEMS, of 1-10-80, which establishes uniform requirements, policies, and responsibilities for the development and implementation of a Department of Energy program to ensure the security of information stored in classified automatic data processing systems.

---

DISTRIBUTION:  
All Departmental Elements  
Federal Energy Regulatory Commission

INITIATED BY:  
Office of Safeguards and Security



- g. DOE 5300.3, TELECOMMUNICATIONS: COMMUNICATIONS SECURITY, of 10-27-80, which establishes the DOE communications security program and implements the provisions of the national policy which are applicable to communications security.
- i. DOE Procurement Regulation 9-50.704.1, which specifies the responsibilities of DOE contractors in the protection of classified information.
- f. DOE 1240.1, MANAGEMENT AND CONTROL OF FOREIGN INTELLIGENCE, of 7-6-78, which establishes responsibilities and authorities of all DOE foreign intelligence activities.

#### 4. DEFINITIONS.

- a. Operations Security (OPSEC). An unclassified term referring to computer, technical, and counterintelligence security measures developed and implemented to augment traditional security programs (physical security, information or personnel security, and communications security). A systematic means of eliminating or controlling vulnerabilities that impact on classified or unclassified technical programs, by reviewing operations so that information of intelligence value (including unclassified information) is not inadvertently provided to an adversary.
- b. Counterintelligence. Intelligence activity, with its resultant product, intended to detect, counteract, and/or prevent espionage and other clandestine intelligence activities, sabotage, or international terrorist activities on behalf of foreign powers, organizations, or persons; it does not include personnel, physical, document, or communications security programs.
- c. Computer Security. The computer-driven aspect of automatic data processing systems security, encompassing the mechanisms and techniques that control access to or use of the computer, or information contained in or handled by it.
- d. Emanations Security (EMSEC). The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from intercept and analysis of compromising emanations from other than crypto-equipment and telecommunications systems.
- e. Emission Security. The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems.
- f. Technical Security. Those measures taken to prevent and detect efforts to acquire classified or sensitive information by technical surveillance. Technical security includes audiocountermeasures, communications security, and prevention or suppression of compromising emissions and emanations.

- g. TEMPEST. An unclassified short name referring to investigations and studies of compromising emanations. It is sometimes used synonymously for the term "compromising emanations," i.e., TEMPEST test, TEMPEST inspections.
5. POLICY. Adequate operations security measures shall be developed and implemented for all existing and planned DOE facilities engaged in activities that impact classified or unclassified information protective measures.
6. RESPONSIBILITIES AND AUTHORITIES.
- a. Assistant Secretary for Defense Programs (DP-1) provides overall management of the operations security program within DOE.
  - b. Director of Safeguards and Security (DP-30).
    - (1) Develops and establishes DOE-wide operations security guidance and instructions by publishing a classified operations security procedural guide. The guide establishes techniques and procedures for the conduct of multidisciplinary operations security activities.
    - (2) Represents DOE in national matters concerning operations security including counterintelligence, computer security, and technical security [for other than communications (COMSEC), transmission, and emissions security].
    - (3) Manages the DOE operations security program by:
      - (a) Planning and programming multidisciplinary support activities.
      - (b) Providing oversight management of operations security surveys.
      - (c) Ensuring that the Headquarters operations security working group, chaired by the Office of Safeguards and Security, represents appropriate program offices and, as necessary, field organizations and other entities such as power marketing administrations and Strategic Petroleum Reserve Office representatives to provide an active forum to discuss and assess generic and specific operations security concerns.
    - (4) Reviews and approves or disapproves all liaison with members of the intelligence community within the Washington, D.C., area on operations security matters.
    - (5) Serves as the DOE central office of record for operations security, excluding communications security, transmission, and emission security.
    - (6) Serves as cognizant office for control of Germantown, Maryland, Sensitive Compartmented Information Facility.

- (7) Manages operations security at the Headquarters level by:
- (a) Instituting and managing operations security procedures and programs, to include an operations security working group to assist in management of Headquarters operations security surveys.
  - (b) Coordinating with field offices on operations security matters and providing assistance as required.
  - (c) Analyzing vulnerabilities detected in the course of Headquarters operations security surveys and developing countermeasures as appropriate.
- c. Assistant Secretary, Management and Administration (MA-1) Through the Director of Computer Services and Telecommunications Management (MA-60).
- (1) Responsible for communications security (COMSEC), transmission, and emission security.
  - (2) Represents DOE in matters concerning communications security, transmission, and emission security.
  - (3) Assists in determining alternative solutions to any telecommunications vulnerabilities detected in the course of an operations security survey. Determines the course of action to correct these vulnerabilities.
- d. Assistant Secretary for International Affairs (IA-1) Through the Deputy Assistant Secretary for International Intelligence Analysis (IA-40). Reviews and approves all DOE-wide guidance, instructions, plans, and procedures concerning the protection of intelligence and intelligence sources and methods.
- e. Managers of Operations Offices.
- (1) Institute, modify, and manage operations security procedures or programs at their respective locations, to include establishing operations security working groups to assist in the management of field operations security surveys.
  - (2) Coordinate with other operations offices on any proposed operations security initiatives that would involve their organization(s) and advise DP-30 accordingly.
  - (3) Develop and maintain operations security program files which consist of operations security program assessments, as required, to assist in developing an active operations security program for critical operations falling within the purview of each field organization.

- (4) Appoint a representative as operations security coordinator to manage operations security procedures and ensure that operations security information promulgated by DP-30 is properly safeguarded and disseminated to authorized recipients with a valid need to know.
- (5) Provide DP-30 a copy of any operations security plan or changes thereto requiring Headquarters interface or assistance.
- (6) Analyze vulnerabilities detected in the course of operations security surveys and develop countermeasures as appropriate.



William S. Heffelfinger  
Assistant Secretary  
Management and Administration