Department of Energy

Washington, D.C.

ORDER

DOE O 470.1

Approved: 9-28-95
Sunset Review: 9-29-97
Expires: 9-29-99
Change 1: 6-21-96

SUBJECT: SAFEGUARDS AND SECURITY PROGRAM

1. OBJECTIVES.

a. To ensure appropriate levels of protection against unauthorized access; theft, diversion, loss of custody, or destruction of nuclear weapons, or weapons components; espionage; loss or theft of classified matter or Government property; and other hostile acts that may cause unacceptable adverse impacts on national security or on the health and safety of Department of Energy (DOE) and contractor employees, the public, or the environment.

b. To deter, prevent, detect, and respond to unauthorized possession, use, or sabotage of special nuclear materials.

c. To provide an integrated system of activities, systems, programs, facilities, and policies for the protection of classified information, nuclear materials, nuclear weapons, nuclear weapons components, and DOE and certain DOE contractor property and personnel as required by the Atomic Energy Act of 1954, as amended, other Federal statutes, Executive orders, and other directives.

d. To use the Design Basis Threat Policy, issued by the Director of Security Affairs, in the design and implementation of protection programs.

e. To provide levels of protection in a graded manner in accordance with the potential risks.

f. To establish safeguards and security programs comparable in effectiveness to other Federally regulated programs with similar interests when such levels are consistent with DOE protective needs and national security interests.

g. To ensure effective planning of graded protection levels and prudent application of resources.

h. To ensure personnel receive training appropriate for their roles in support of the program and that persons given access authorization are aware of Safeguards and Security Program requirements.

i. To standardize safeguards and security equipment and systems to achieve operational and financial benefits.

2. CANCELLATIONS. The Orders listed below are canceled. Cancellation of an Order does not, by itself, modify or otherwise affect any contractual obligation to comply with such an Order. Canceled Orders which are incorporated by reference in a contract shall remain in effect until the contract is modified to delete the reference to the requirements in the canceled Orders.

   a. DOE 5630.11B, SAFEGUARDS AND SECURITY PROGRAM, of 8-2-94.

   b. DOE 5630.13A, MASTER SAFEGUARDS AND SECURITY AGREEMENTS, of 6-8-92.

   c. DOE 5630.14A, SAFEGUARDS AND SECURITY PROGRAM PLANNING, of 6-9-92.

   d. DOE 5630.15, SAFEGUARDS AND SECURITY TRAINING PROGRAM, of 8-21-92.

   e. DOE 5630.16A, SAFEGUARDS AND SECURITY ACCEPTANCE AND VALIDATION TESTING PROGRAM, of 6-3-93.

   f. DOE 5630.17, SAFEGUARDS AND SECURITY (S&S) STANDARDIZATION PROGRAM, of 9-29-92.

   g. DOE 5631.1C, SAFEGUARDS AND SECURITY AWARENESS PROGRAM, of 5-4-94.

   h. DOE 5631.4A, CONTROL OF CLASSIFIED VISITS, of 7-8-92.

   i. DOE 5634.1B, FACILITY APPROVALS, SECURITY SURVEYS, AND NUCLEAR MATERIALS SURVEYS, of 9-15-92.

   j. DOE 5634.3, FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE PROGRAM, of 6-14-93.

   k. DOE 5639.3, VIOLATION OF LAWS, LOSSES, AND INCIDENTS OF SECURITY CONCERNS, of 9-15-92.

   l. Chapter XI, "Protection Element: Acceptance and Validation Testing," in DOE M 5632.1C-1, MANUAL FOR PROTECTION AND CONTROL OF SAFEGUARDS AND SECURITY INTERESTS, of 7-15-94.

3. APPLICABILITY.

   a. DOE Elements. DOE Elements responsible for safeguards and security activity and/or the protection and control of safeguards and security interests.

   b. Contractors. Except for the exclusions in paragraph 3c, the Contractor Requirements Document (Attachment 1) sets forth requirements that are to be applied to the covered contractors.

c. Exclusions. DOE facilities and activities regulated by the Nuclear Regulatory Commission.

4. REQUIREMENTS. General Safeguards and Security Program requirements are listed below and in the chapters appended to this Order. Detailed requirements for personnel security activities, protection operations, information security, and materials control and accountability are set forth in the Orders listed in subparagraph a below. Note that terms commonly used in the Safeguards and Security Program are defined in the "Safeguards and Security Definitions Guide," which is maintained by the Office of Safeguards and Security.

a. Key Safeguards and Security Program Elements.

(1) Program Management, DOE O 470 series.

(2) Personnel Security, DOE O 472 series.

(3) Protection Operations, DOE 5632 and DOE O 473 series.

(4) Materials Control and Accountability, DOE 5633 and DOE O 474 series.

(5) Information Security, DOE 5639 and DOE O 471 series.

b. Risk Management. The determination of the appropriate level of protection against risk shall consider the nature of the threat, the vulnerability of the potential target, and the potential consequences of an adversarial act. Accordingly, safeguards and security programs shall be based on vulnerability/risk analyses designed to provide graded protection in accordance with the asset's importance or the impact of its loss, destruction, or misuse. Risks to be accepted by the Department shall be identified and documented by vulnerability/risk analyses.

c. Graded Protection. By graded approach, DOE intends that the highest level of protection be given to security interests whose loss, theft, compromise, and/or unauthorized use will seriously affect the national security, and/or the health and safety of DOE and contractor employees, the public, the environment, or DOE programs. Protection of other interests shall be graded accordingly. Asset valuation, threat analysis, and vulnerability assessments shall be considered, along with the acceptable level of risk and any uncertainties, to decide how great is the risk and what protection measures are to be applied.

It should be recognized that risks will be accepted (i.e., that actions cannot be taken to reduce the potential for or consequences of all malevolent events to zero); however, an acceptable level of risk will be determined based on evaluation of a variety of facility-specific goals and considerations. Protection-related plans shall describe, justify, and document the graded protection provided the various safeguards and security interests.

d. Site-Specific Programs. Safeguards and security programs shall be tailored to address site-specific characteristics.

e. Planning. Chapter I sets forth detailed requirements for site-wide plans to be developed and maintained at the Operations Office, or equivalent-level, and for other plans to address specific needs.

f. Deviations. Alternate or equivalent means of providing adequate safeguards and security may be proposed to meet a specific requirement of this and other Safeguards and Security Program directives. In some cases, it may be justifiable not to meet a requirement by any means. The following procedures and approval levels shall apply to all such deviations from Safeguards and Security Program directives' requirements. Any extensions to the approved period of time for deviations shall require reapplication for approval.

(1) Variances are approved conditions that technically vary from a Safeguards and Security directive's requirement, but afford equivalent levels of protection without compensatory measures.

(a) Variances shall be approved by the Head of a Field Element. The Office of Safeguards and Security and appropriate program offices shall be notified.

(b) For Headquarters Elements, the cognizant Secretarial Officer shall approve variances with the concurrence of the Director, Headquarters Operations Division, Office of Safeguards and Security.

(c) Variances may be approved for an indefinite period.

(2) Waivers are approved nonstandard conditions that deviate from a Safeguards and Security directive's requirement which, if uncompensated, would create a potential or real safeguards and security vulnerability. Waivers therefore require implementation of compensatory measures for the period of the waiver (e.g., expenditure of additional resources to implement enhanced protection measures).

(a) Waivers shall be approved by Heads of Field Elements provided:

1 the cognizant Secretarial Officer(s) and the Office of Safeguards and Security are notified 30 days in advance of such approval;

2 comments provided by Headquarters Elements are considered before approving the waiver;

3 adequate compensatory measures are in place; and

4 performance testing is accomplished, if appropriate.

(b) Waivers for Headquarters Elements may be approved by the cognizant Secretarial Officer providing:

1 the Office of Safeguards and Security is notified 30 days in advance of approval and the Director, Headquarters Operations Division has concurred in the waiver; and

2 the requirements of subparagraphs 4f(2)(a)3 and 4 above are met.

(c) A waiver shall not exceed 2 years. Extensions may be requested using the same process.

(3) Exceptions are approved deviations from a Safeguards and Security directive's requirement that create a safeguards and security vulnerability. Exceptions shall be approved only when correction of the condition is not feasible and compensatory measures are inadequate to preclude the acceptance of risk. An exception must be approved by both the Secretarial Officer and the Director of Security Affairs.

(a) For Field Elements, exception requests shall be submitted through line management to the cognizant Secretarial Officer and to the Director of Security Affairs for review and approval.

(b) For Headquarters Elements, exception requests shall be submitted through the Headquarters Operations Division for review and approval by the cognizant Secretarial Officer and the Director of Security Affairs.

(c) Exceptions shall not exceed 3 years. Extensions may be requested using the same process.

(d) The need for an exception shall be validated annually.

(e) Exceptions shall be included in Site Profiles, which form the basis for the DOE's Annual Report to the President on the Status of Safeguards and Security.

(4) Documentation. Specific information to be included to document each deviation is provided in Appendix 1. Approved deviations shall be documented in safeguards and security documents. A deviation request approved out of cycle with the safeguards and security plan formulation and approval process shall be documented as an attachment to the applicable safeguards and security plan.

(5) Vulnerability Assessments and Performance Testing. Compensatory measures implemented and used as the basis for an exception request shall be subject to formal vulnerability assessments and must be tested and validated by the cognizant Field Element. The

results of the vulnerability assessment(s) and tests shall be documented in the applicable security plan. Performance testing and documentation, as necessary, may also be required for waivers.

(6) Visits. Office of Safeguards and Security and affected program office representatives may perform on-site reviews, assessments, and validation visits to ascertain the nature and impact of deviation requests.

(7) Corrective Actions. Heads of DOE Elements shall monitor corrective actions, establish schedules, ensure that funding is effectively managed to address safeguards and security interests, and monitor compliance with schedules.

g. Standardization.

(1) Safeguards and security equipment and systems shall be selected on the basis of providing a benefit to DOE such as worker safety, compliance with life safety codes, enhancing mission capability, cost advantages, or facilitating contingency efforts.

(2) New facility designs shall incorporate the use of standardized safeguards and security equipment and systems where possible without compromising design flexibility or adherence to performance criteria.

h. Management Review of Safeguards and Security Programs. Individuals assuming Head of Field Element positions shall complete a status review for their safeguards and security programs. Within 15 calendar days of the review, a written report that identifies any significant deficiencies and corrective actions being taken or planned shall be sent to the Under Secretary or cognizant Program Office, as appropriate, with a copy to the Director of Security Affairs.

5. RESPONSIBILITIES.

a. Secretarial Officers.

(1) Provide program and project direction consistent with the Safeguards and Security directives and policy requirements.

(a) In coordination with the Director of Nonproliferation and National Security.

1 Ensure adequate protection is afforded safeguards and security interests.

2 Establish action criteria, including curtailment or suspension of operations, for operations that would result in an immediate and unacceptable risk to national security, the health and safety of employees, the public, or the environment.

(b) Coordinate construction or alteration projects of facilities having a safeguards or security interest with the Director of Security Affairs and the Associate Deputy Secretary for Field Management.

(c) Request establishment of safeguards and security activities and facility clearance(s) through the Office of Safeguards and Security. Notify the Office of Safeguards and Security to terminate registration of such activities and facility clearances.

(2) Implement a security program consistent with the Headquarters Security Plan for Washington, D.C. area facilities and programs.

(3) Approve or disapprove requests for exceptions from Safeguards and Security directives' requirements in accordance with paragraph 4f(3)(a) to (e).

(4) Ensure that each request for a procurement requiring application of this Order incorporates the requirements specified in the Contractor Requirements Document (Attachment 1).

(a) Designate individual(s) to notify contracting officers of each procurement falling within the scope of this Order. Unless another individual is designated, the responsibility is that of the procurement request originator (the individual responsible for initiating a requirement on DOE F 4200.33, "Procurement Request Authorization").

(b) Ensure the following:

1 The contracting officer provides DOE F 5634.2, "Contract Security Classification Specification," to the servicing safeguards and security office.

2 The contract clauses set forth in the DOE Federal Acquisition Regulation and other relevant sections of 48 CFR Chapter IX are included in contracts, as applicable.

3 The contracting officers incorporate provisions implementing the requirements of this Order in new and existing contracts that involve access authorizations, classified information, nuclear and other hazardous material presenting a potential radiological or toxicological sabotage threat, or Departmental property valued at more than $5,000,000.

4 Contractual coverage is in place to permit implementation of this Order with regard to the contractor's nuclear materials activities before

initiation of any action involving nuclear materials with a license-exempt (as defined in 10 CFR Part 50) contractor.

5 Non-DOE funded work under their jurisdiction is provided protection in accordance with the Departmental safeguards, security, and classification policies.

(c) Appoint within their contracting activity a trained DOE employee as the Foreign Ownership, Control, and Influence (FOCI) point-of-contact.

(5) Ensure that safeguards and security budget proposals are adequate, and that resources are provided to implement them.

(6) Participate in the development and review of policy and standards for safeguards and security interests.

(7) Identify technological needs to the Office of Security Affairs for consideration in the safeguards and security technology development program.

(8) Implement the Classified Visits Program in accordance with Chapter VIII.

(a) Designate specific facilities where visits may be made only with the approval of the organization having program responsibility, and inform Heads of DOE Elements.

(b) Maintain records of individuals approved by their organizations to have continuing access on the basis of DOE Q and L access authorizations or Department of Defense or National Aeronautics and Space Administration certifications, and notify the Director of Safeguards and Security when such approvals are granted or canceled.

(9) Approve Site Safeguards and Security Plans and annual revisions thereto.

b. The Director of Nonproliferation and National Security shall, in addition to the duties shown in paragraph 5a, direct and coordinate the policy and procedures for a comprehensive Safeguards and Security Program.

(1) Through the Director of Security Affairs.

(a) Establish safeguards and security policies, requirements, standards, and guidance for DOE operations, including design basis threat, for use in designing and implementing DOE protection programs.

(b) Provide advice and assistance concerning safeguards and security programs, and coordinate with appropriate DOE organizations to correct safeguards and security deficiencies.

(c) Approve all Site Safeguards and Security Plans, and participate in validation and verification reviews at field sites.

(d) Establish and maintain the DOE Declassification Program and ensure consistency between classification and safeguards and security policies.

(e) Serve as DOE's central point for coordination and liaison with other agencies, groups, and DOE Elements in the development and execution of an effective Safeguards and Security Program.

(f) Coordinate with DOE Elements in the recommended curtailment or suspension of operations at DOE facilities when continuation of such operations would result in an unacceptable risk to national security, the health and safety of employees, the public, or the environment. Suspend the facility clearance where the level of the facility's safeguards and security program has significant vulnerability, unacceptable risk, or inadequate protection, and approve removal of facility clearance. Reinstate facilities when satisfactory conditions exist. Notify other Federal agencies having concurrent safeguards or security interests of suspension or reinstatement actions.

(g) Advise Program Offices on their safeguards and security requirements and budgets before DOE approval. Ensure differences identified through the review process are resolved during DOE's internal review budgeting process (or equivalent process for reprogramming actions).

(h) Through the Director of Safeguards and Security.

1 Serve as the DOE focal point for safeguards and security matters.

2 Formulate policies, procedures, and plans to ensure the effective and efficient protection of nuclear materials, classified information, and DOE property and facilities.

a Base policies, procedures, and plans on the design basis threat requirements, standards, and guidelines.

b Provide, as requested, advice and assistance to Secretarial Officers and Heads of Field Elements in the implementation of safeguards and security requirements.

c Act as DOE's focal point for the collection, retention, evaluation, and dissemination of information of safeguards and security significance, including threat assessment and protection systems data.

d Develop and maintain guidelines for Site Safeguards and Security Plans, in consultation with affected DOE Elements.

e Establish safeguards and security policy and training quality panels.

f Approve or disapprove exceptions in accordance with paragraph 4f(3(a) to (e).

3 Provide focus for interagency matters pertaining to safeguards and security, including wartime protection planning and law enforcement; provide liaison with the Nuclear Regulatory Commission, Federal Bureau of Investigation, Department of Defense, and other Federal law enforcement and security agencies.

4 Recommend suspension of the facility clearance of any facility whose safeguards and security program is unacceptable in meeting minimum safeguards and security protection levels and associated risk.

5 Direct the safeguards and security technology development program to support user needs and policy objectives.

6 Participate in staffing line-item construction project actions for prioritizing projects through validation of specific projects and participate in program office Change Control Board actions.

7 Consolidate and coordinate the Annual Report to the Secretary on the Safeguards and Security Status.

8 Ensure development, conduct, and management of an effective Safeguards and Security Training Program.

a Develop and issue policy for safeguards and security training programs and coordinate with the Assistant Secretary for Human Resources and Administration to ensure conformance with DOE training policy.

b. Provide and manage personnel and budget resources for a standardized training program at the Safeguards and Security Central Training Academy.

c. Ensure that a safeguards and security Training Approval Program is developed, implemented, and administered.

d. Conduct annual reviews of safeguards and security training programs DOE-wide and report findings as part of the annual report to the Secretary.

e. Approve certifications that local safeguards and security training programs meet DOE standards.

9. Ensure the development, implementation, and management of an effective Safeguards and Security Awareness Program.

10. Oversee implementation of the Classified Visits Program.

a. Obtain and review security assurances to determine consistency with agreements for cooperation and other international agreements, when applicable.

b. Maintain a current list of all Department of Defense and National Aeronautics and Space Administration officials authorized to certify personnel under their jurisdiction for access to Restricted Data, and provide such lists to DOE Elements.

c. Help identify Heads of DOE Elements and Federal officials to whom specific requests for visits should be directed.

d. Approve requests for classified visits involving safeguards and security programmatic matters.

e. Certify on DOE F 5631.20, "Request for Visit or Access Approval," the DOE access authorization type, number, and date for individuals possessing a DOE Headquarters access authorization in those instances in which this form is required.

11. Maintain the Safeguards and Security Information Management System.

12. Ensure the development, implementation, and management of an effective Facility Survey and Clearance Program.

a Designate a trained Facility Survey and Clearance Program Manager (a DOE employee).

b Approve extended survey schedules for facilities with Category I quantities of special nuclear material.

13 Ensure the development, implementation, and management of an effective FOCI.

a Designate a trained FOCI Program Manager (a DOE employee).

b In coordination with General Counsel, when appropriate, provide a favorable FOCI determination to the Lead Responsible Office.

14 Through the Director of Safeguards and Security Central Training Academy, manage the Academy to achieve program objectives expressed in Chapter II.

15 Through the Director, New Brunswick Laboratory.

a Manage the Laboratory to achieve program objectives.

b Provide state-of-the-art services for measurement of nuclear materials in support of DOE safeguards requirements.

c Assess the effectiveness of DOE facility materials measurement processes and materials control and accountability programs.

d Provide certified reference materials ensuring traceability of DOE nuclear materials measurements to a national and international measurements data base.

(i) Through the Director of Declassification, arrange and approve classified visits of foreign nationals sponsored by a foreign government to the Office of Declassification in connection with the information classification programs, and refer security assurances to the Office of Safeguards and Security.

(2) Through the Director of Energy Intelligence.

(a) Appoint a Special Security Officer for line management security administration of DOE's Sensitive Compartmented Information Facilities.

(b) Provide accreditations, in coordination with the Office of Safeguards and Security, that planned/installed physical and technical security systems create an environment of acceptable risk for intelligence-related facilities.

(c) Serve as DOE's point-of-contact involving intelligence and counterintelligence activities, to include management of program access. Coordinate with the Director of Security Affairs concerning security issues, including espionage and the potential compromise of intelligence-related information.

(3) Through the Director of Emergency Management, provide timely and current intelligence threat information to support the Safeguards and Security Program.

c. The Assistant Secretary for Environment, Safety and Health, through the Deputy Assistant Secretary for Oversight.

(1) Maintain an inspection, performance testing, and evaluation program that, in accordance with DOE 5630.12A, SAFEGUARDS AND SECURITY INSPECTION AND ASSESSMENT PROGRAM, provides independent oversight of the Department's Safeguards and Security Program.

(2) Ensure participation with the Department of Defense in conducting joint ATOMAL inspections to verify that Restricted Data and Formerly Restricted Data released by the United States to NATO and NATO member nations as ATOMAL information is being protected appropriately.

(3) Ensure all NATO/ATOMAL Control Points and Subcontrol Points are inspected to verify NATO and ATOMAL holdings are being appropriately protected.

d. Assistant Secretary for Defense Programs shall, in addition to the responsibilities in paragraph 5a, support the Classified Visits Program by appointing an approval authority for requests for visits requiring access to the following:

(1) Nuclear weapon information concerned with the design, manufacture, or use of atomic weapons, atomic weapon components, or atomic explosive devices; and nuclear weapon information in connection with the military application of atomic energy under sections 144b and c(1) and 91(c) or (4) of the Atomic Energy Act of 1954, as amended. (NOTE: Approval authority will be responsible for obtaining endorsements for programmatically controlled access for specific nuclear weapon information.)

(2) Nuclear materials production facilities or access to sensitive nuclear materials production information, excluding classified uranium enrichment technology .

(3) Classified production facilities, excluding visits for classified uranium enrichment technology, by employees of other Federal agencies, their contractors, or subcontractors.

e. Assistant Secretary for Human Resources and Administration shall establish programs and training for communications security, electronic emissions control (emissions security), and unclassified computer security.

f. Deputy Assistant Secretary for International Energy Policy shall serve as approval authority, in concert with appropriate Headquarters program staff, for classified visits by foreign nationals.

g. Associate Deputy Secretary for Field Management.

(1) Ensure strategic planning is completed for all Field Elements and conduct management coordination and oversight of multi-purpose Operations Offices as they impact the Safeguards and Security Program planning process.

(2) Ensure requirements for physical protection of facilities are incorporated into construction contracts.

h. The Director, Office of Nuclear Energy, through the Director of Uranium Programs, shall approve requests for visits involving access to uranium enrichment plants and to facilities engaged in uranium enrichment technology development, including gaseous diffusion, gas centrifuge, and advanced isotope separation technologies. (Managers of Field Elements may approve visits to facilities under their jurisdiction for contractors requiring access because of their continuing programmatic association or for contractor personnel administered under contracts with the Field Elements.)

i. Director, Naval Nuclear Propulsion Program, shall implement and oversee all policy and practices pertaining to this Order for activities under the Director's cognizance.

j. Heads of Field Elements shall ensure that all operations under their jurisdiction are implemented consistent with acceptable safeguards and security practices and in accordance with the Safeguards and Security directives.

k. Albuquerque, Chicago, Idaho, Nevada, Oak Ridge, Richland, Oakland, and Savannah River Operations Offices; Pittsburgh and Schenectady Naval Reactors; Rocky Flats Office; Strategic Petroleum Reserve Office; and the Office of Safeguards and Security, Headquarters Operations Division.

(1) Lead Responsible Offices.

(a) Ensure safeguards and security surveys of facilities under their purview are conducted.

(b) Establish written delegations of authorities and responsibilities for administration of the facility survey, registration and clearance, and FOCI programs.

(c) Designate a Facility Clearance Operations Manager (DOE employee) to manage the local program.

(d) Designate a FOCI manager (DOE employee) to manage the local program.

(e) Ensure the designation of a trained DOE employee as the FOCI point of contact in each contracting/procurement organization.

(f) Ensure the designation of a trained DOE employee as the FOCI point of contact in the Chief Counsel office.

(g) Develop local implementing procedures for the facility survey, registration and clearance, and FOCI programs.

(h) Grant approval for facilities and register safeguards and security activities.

(i) Terminate facility clearances and registrations of safeguards and security activities under their cognizance.

(j) Maintain information in the Safeguards and Security Information Management System for all facilities for which they are either the Lead Responsible Office or at which they have registered a safeguards and security activity.

(k) Ensure affected Departmental Elements are notified when an activity is suspended or terminated.

(l) Provide written notification to an approved facility whenever there is a change in the Lead Responsible Office.

(2) Surveying Offices.

(a) Ensure that an effective program is instituted to plan, conduct, and follow up safeguards and security surveys and self-assessments.

(b) Designate a Facility Survey Operations Manager (a DOE employee).

(c) Develop local implementing procedures for the administration and conduct of surveys and self-assessments.

(d) Provide input to the Safeguards and Security Information Management System current data for all surveyed facilities.

(e) Provide sufficient resources for the survey program to support professional, administrative, technical, and clerical staffing requirements, equipment and materials, logistics requirements, and training and development.

(f) Ensure that prior to working independently, persons assigned to perform survey and review duties possess appropriate knowledge, skills, and ability.

l. General Counsel.

(1) Appoint a trained DOE employee to serve as the FOCI point-of-contact.

(2) Upon request by the Office of Safeguards and Security, ensure review of all complex FOCI cases; e.g., FOCI cases involving Proxy Agreements and Voting Trusts.

m. Procurement Request Originators are the individuals responsible for initiating a requirement on DOE F 4200.33, "Procurement Request Authorization," or such other individuals(s) as designated by cognizant Heads of DOE Elements. Procurement Request Originators shall notify the cognizant contracting officers of the following:

(1) Each procurement requiring the application of this Order.

(2) Requirements for flow-down of this Order to any subcontract or subaward.

(3) Identification of the paragraphs or other portions of this Order with which the awardee or, if different, a subawardee is to comply.

n. Contracting Officers at all levels shall:

(1) Incorporate contract provisions implementing the applicable requirements of Safeguards and Security directives in new or existing contracts, and

(2) Not award contracts requiring access authorizations until a Facility Clearance is granted.

6. CONTACT. Comments and inquiries may be directed to the Materials Control and Accountability Program Manager, 301-903-2536, or to the points of contact provided in the chapters.

BY ORDER OF THE SECRETARY OF ENERGY:

ARCHER L. DURHAM
Assistant Secretary for
Human Resources and Administration

DEVIATION REQUEST FORMAT

1. Date. Date the request is signed by the requesting official.

2. Request Number. Alphanumeric identifier beginning with "OSS," followed by the routing symbol used in the DOE National Telephone Directory, followed by the last two digits of the year in the request's date, followed by the three-digit number that is next in the sequence of requests from that Field Element in that calendar year. For example, the third request from Albuquerque Operations Office during 1995 would be OSS-AL-95-003.

3. Directive Citation. Title and date of the directive from which a deviation is being requested with a citation (paragraph or other provision) and summary of the directive's requirement.

4. Impacted Entity. Identification of the specific facility (Safeguards and Security Information Management Systems facility code number), process, procedure, system, etc.

5. Deviation Justification. Specific description of the deviation and the associated reason or rationale for the deviation request. A description of the relationship of the subject of the deviation request to other safeguards and security interests shall be included if they are significantly affected.

6. Protection Measures. Description of the current measure(s) used for protection and an evaluation of the effectiveness of such measure(s); description of alternate/compensatory measure(s) or level(s) of protection to be provided as an alternative to the Order requirement(s).

7. Duration. Expected duration of the condition for which the deviation is requested, including milestones for correcting, alleviating, or eliminating the deviant condition, if applicable. (Note: Waivers cannot be for more than 2 years; exceptions cannot be for more than 3 years.)

8. Risks. Evaluation of the risk associated with the deviation, if approved. Results of vulnerability analyses and performance tests conducted on proposed alternative(s) shall be included.

9. Signature. Requesting official's signature.

TABLE OF CONTENTS

CHAPTER IX - SURVEY PROGRAM

CHAPTER X - SELF-ASSESSMENT PROGRAM

CHAPTER I

SAFEGUARDS AND SECURITY PROGRAM PLANNING

1. OBJECTIVE. To establish a standardized approach to protection program planning that will provide an information baseline for use in integrating complex-wide safeguards and security considerations, facilitate managers' evaluation of program elements and resources for needed improvements, and establish cost-benefit bases for analyses and comparisons.

2. APPLICABILITY. This chapter applies to the following DOE-owned and -leased sites and facilities and to covered contractor-owned and -leased facilities.

   a. Those that have Category I quantities of special nuclear materials, or those that have Category II quantities within the same Protected Area that roll up to a Category I quantity.

   b. Those that have a radiological/toxicological sabotage threat that would cause an unacceptable impact on the national security, the health and safety of employees, the public, or the environment.

   c. Those that have an industrial sabotage threat that would cause an unacceptable impact to those DOE programs supporting national defense and security.

   d. Those facilities engaged in intra-site transportation of special nuclear materials.

   e. Those facilities possessing classified matter.

   f. Those facilities engaged in the protection of government property.

   g. Other facilities/sites that Heads of DOE Elements deem appropriate.

3. PLANNING REQUIREMENTS. The following topics shall be essential elements for planning safeguards and security programs.

   a. Site-Specific Characteristics. Protection programs shall be tailored to address specific site characteristics and requirements, current technology, ongoing programs, and operational needs, and to achieve acceptable protection levels that reduce inherent risks on a cost-effective basis.

   b. Threat. The "Design Basis Threat Policy for the Department of Energy (DOE) Programs and Facilities (U)" shall be used with local threat guidance and vulnerability assessments for protection and control program planning.

   c. Protection Strategy.

(1) Strategies for the physical protection of special nuclear materials and vital equipment shall incorporate the applicable requirements established in DOE M 471.2, MANUAL FOR CLASSIFIED MATTER PROTECTION AND CONTROL.

(a) Protection strategy may be graduated to address varying circumstances and may range from denial to containment to recapture/recovery to pursuit.

(b) A denial strategy shall be used for the protection of Category IA special nuclear materials and certain radiological sabotage targets where unauthorized access presents an unacceptable risk.

(c) Programs shall be designed to prevent unauthorized control (i.e., an unauthorized opportunity to initiate or credibly threaten to initiate a nuclear dispersal or detonation, or to use available nuclear materials for onsite assembly of an improvised nuclear device).

(d) A containment strategy shall be used to prevent the unauthorized removal of Category II or greater special nuclear materials.

(e) Should denial and/or containment fail, a recapture/recovery or pursuit strategy would then be required.

(f) Forces shall be capable of rapid reaction in implementing recapture or recovery contingencies.

(g) Programs must be designed to prevent acts of radiological/toxicological sabotage that would cause unacceptable impact to national security or pose significant dangers to the health and safety of employees, the public, or the environment, and/or mitigate the consequences of acts of radiological/toxicological sabotage that would cause unacceptable impact to national security or pose significant dangers to the health and safety of employees, the public, or the environment.

(2) Strategies for the protection and control of classified matter shall incorporate the applicable requirements established in DOE M 5632.1C-1, MANUAL FOR PROTECTION AND CONTROL OF SAFEGUARDS AND SECURITY INTERESTS; DOE M 5639.6A-1, MANUAL OF SECURITY REQUIREMENTS FOR THE CLASSIFIED AUTOMATED INFORMATION SYSTEM SECURITY PROGRAM; and DOE M 471.2-1, MANUAL OF SECURITY REQUIREMENTS FOR THE CLASSIFIED AUTOMATED INFORMATION SYSTEM SECURITY PROGRAM. Security systems shall be used that detect or deter unauthorized disclosure, modification, or the loss of availability of classified and sensitive, but unclassified, information and its unauthorized removal from a site or facility.

(3) Strategies for the protection of Government property not covered in subparagraphs (1) and (2) above shall reflect a graded approach.

(4) Security countermeasures to address bombings shall consider a range of activities from hand-carried, mailed, and vehicle-transported devices.

d. Graded Protection. Protection-related plans shall describe, justify, and document the graded protection provided the various safeguards and security interests.

4. PLANNING.

a. Site Safeguards and Security Plan. This plan is an Operations Office or equivalent-level master planning document that shall be prepared for sites with facilities described in paragraphs 2a, 2b, 2c, and 2g. The plan shall depict the existing condition of safeguards and security sitewide and by facility, and shall establish improvement priorities and resource requirements for the necessary improvements. Plans shall contain information that describes:

(1) protection strategies;

(2) site/facility safeguards and security programs in place and/or planned;

(3) plans and procedures designed to implement, manage, and maintain safeguards and security programs;

(4) resources needed to sustain the site protection program in its current configuration and during planning revisions;

(5) security staff personnel qualifications as outlined in approved position descriptions and/or prescribed in DOE directives;

(6) the results of vulnerability analyses and risk assessments:

(a) levels of acceptable risks;

(b) assumptions established and used as part of the vulnerability assessment process;

(c) validation of vulnerability analyses results by performance testing;

(7) required corrective actions and how those actions will mitigate identified vulnerabilities and reduce residual risk;

(8) sources of supporting documentation detailing where planning assumptions, relative to the facility, the adversary, and the DOE national security mission can be found; and

(9) approved deviations.

b. Security Plans. At locations where a Site Safeguards and Security Plan is not required due to the limited scope of safeguards and security interests, a security plan shall be developed to describe the protection program in place. In addition, specialized plans shall be developed to address protection programs for classified automated information systems, materials control and accountability, and other protection operations. Requirements for specialized plans that may or may not be components of Site Safeguards and Security Plans are set forth in the applicable DOE O 470 and 5630 series of directives.

(1) Materials Control and Accountability Plans. See DOE 5633.3B, CONTROL AND ACCOUNTABILITY OF NUCLEAR MATERIALS, of 9-7-94, for requirements for this type of plan.

(2) Classified Automated Information System (AIS) Security Plans. See DOE M 5639.6A-1 for requirements for this type of plan.

c. Planning Inputs. The following documents shall be used to support program forecasts and information input used in the protection program planning process.

(1) Current DOE directives, DOE threat guidance, and applicable intelligence assessment information developed and disseminated by Headquarters Elements.

(2) Programmatic guidance and forecasts of significant changes planned in site operations, as communicated through Heads of Field Elements and appropriate Headquarters Elements.

(3) Current and projected operational constraints and resources.

(4) Protection program policy guidance provided by DOE Elements.

d. Plan Review and Approval.

(1) Heads of Field Elements shall approve and forward Site Safeguards and Security Plans to the applicable program office for coordination. Changes to the Plans that significantly alter the agreed-on protection philosophy or performance standards of protection systems shall require approval by the Head of the Field Element and concurrence by the cognizant program office and the Director of Security Affairs. Other plans shall be approved by the Head of Field Element or as stipulated in the applicable directive.

(2) The Site Safeguards and Security Plan shall be reviewed and updated annually. Copies of modifications and updates will be provided to the Office of Safeguards and Security for review and comment.

5. IMPLEMENTATION ASSISTANCE. The Office of Safeguards and Security will develop and maintain, after appropriate coordination with affected elements, guidelines to assist facilities in safeguards and security planning.

6. CONTACT. Comments and inquiries on this chapter may be directed to the Materials Control and Accountability Program Manager at (301) 903-2536. Inquiries pertaining to implementation may be directed to the Field Operations Division at (301) 903-4243.

CHAPTER II

SAFEGUARDS AND SECURITY TRAINING PROGRAM

1. OBJECTIVE. To train DOE and DOE contractor personnel to a level of proficiency and competence that ensures they are qualified to perform assigned safeguards and security tasks and/or responsibilities, thus providing high assurance that the safeguards and security programs of the Department are successful.

2. APPLICABILITY. This chapter applies to personnel performing tasks and responsibilities addressed in this and other Safeguards and Security directives associated with protecting nuclear weapons, weapons components, special nuclear materials, classified matter, and/or government property.

3. PROGRAM REQUIREMENTS.

   a. The Safeguards and Security Training Program shall encompass training in the following Safeguards and Security Program key elements.

      (1) Program Management.

      (2) Personnel Security.

      (3) Protection Operations.

      (4) Materials Control and Accountability.

      (5) Information Security.

   b. Training methodology and courses shall be standardized. The scope and level of training provided to individuals shall be tailored to their assigned duties and responsibilities and shall be based upon an analysis of their prior safeguards and security experience and training.

   c. Training programs shall be based on the results of job analyses to document the identification and description of major tasks and skill requirements.

   d. Knowledge and performance-based testing shall apply to all required training to measure the skills acquired from the training programs developed.

   e. For specialized skill requirements, such as armorers, personnel security specialists, nuclear materials custodians, and technical surveillance countermeasures technicians, performance testing shall form the primary basis for certification.

f. The Training Approval Program (TAP) is a process to formally recognize safeguards and security training programs that are conducted by an organization other than the Safeguards and Security Training Academy to ensure established objectives, standards, and criteria are met.

(1) A Training Approval Program shall be implemented to ensure standardization of safeguards and security training conducted at DOE facilities other than the Safeguards and Security Central Training Academy. (The "Guide for Implementation of DOE 5630.15, Safeguards and Security Training Program" provides details on Training Approval Program implementation.)

(2) Developed and refined safeguards and security training program objectives, standards, and criteria shall be distributed to facilitate development of training programs.

(3) Site programs shall be examined by representatives of the Office of Safeguards and Security on a recurring basis, but no less than every 3 years, to verify adherence to DOE objectives, standards, and criteria, and to provide program approval recommendations to the Director of Safeguards and Security.

(4) Initial and recurring reviews for training approval shall cover all aspects of local training programs to include program management and structure, course contents, training facilities, observation of course presentations for effectiveness, and evaluation of students.

(5) Instructors shall be evaluated for knowledge in their assigned training area and effectiveness in presenting assigned course materials.

(6) Individuals shall be tested to evaluate skills and knowledge achieved through course participation.

(7) Training approvals shall remain valid for a period of 3 years.

g. Training shall be provided to individuals to qualify or improve their qualifications to perform assigned safeguards and/or security tasks or responsibilities. Initial and refresher training shall be tailored to the required knowledge and skills.

h. The Safeguards and Security Central Training Academy shall provide a state-of-the-art training facility and program, emphasizing training for DOE Element instructors and instructor-candidates, as follows.

(1) Standardization of training in safeguards and security courses and programs through certification of key skill personnel, development of skills enhancement courses, and approval of facility training programs.

(2) Standardization of training courses for the key program elements. Information associated with these training courses would be available to DOE Elements and contractors for use in their training programs.

(3) Standardization of testing procedures to assess proficiency, knowledge, and skills. Associated information would be made available to DOE Elements and contractors.

(4) Development and maintenance of a repository of information pertaining to relevant external sources of training and training materials, as well as data regarding needs that cannot be satisfied by DOE resources.

(5) Maintenance of a library of current and historical reference materials to support all aspects of the training program.

(6) Effective relationships with other Federal training facilities and operational safeguards and security functions to further training objectives.

(7) Review of DOE and contractor safeguards and security training programs to assess adherence to established quality standards in course content and presentation.

i. A Safeguards and Security Training Advisory Committee shall be chaired by the Director of the Central Training Academy.

(1) Members shall include two senior level officials from the Office of Safeguards and Security, two senior officials from DOE Operations Offices who are nominated by the chair and approved by the Director of Safeguards and Security, and two senior contractor personnel to serve as technical advisors. Technical advisors shall be nominated by the chair and approved by the Director of Safeguards and Security. Members and technical advisors shall serve for 2 years or as decided by the Director of Safeguards and Security. The chair of the Committee shall hold meetings at least semi-annually.

(2) The Committee shall:

(a) review, evaluate, and recommend specific subject areas and curriculum content required to establish standardized training;

(b) recommend and assist in obtaining resources required to support the standardized training program;

(c) review the implementation status of safeguards and security training policy and guidance; and

(d) annually review and validate the Central Training Academy's operations, course schedule, course approval and certification procedures, and strategic plans.

j. Central Training Academy instructors shall be certified by the Director of the Academy.

(1) Certification shall remain valid so long as the individual fulfills all required refresher training.

(2) Certification shall be based on a records review of qualifications and a recommendation by the individual responsible for the training program.

(3) Instructors of courses provided by other DOE Elements and contractors shall be certified by the individual responsible for the DOE Element or contractor training program.

k. Development, review, and presentation of training courses for unique site-specific requirements shall be the responsibility of cognizant sites. Course materials shall be available upon request for review and approval by the cognizant Departmental Element and/or the Training Approval Program team.

l. The Central Training Academy, DOE Elements, and covered contractors shall implement a standardized training records management system as described below.

(1) Records shall be maintained to document training provided to personnel participating in the DOE safeguards and security program. Records of training shall contain course identification, dates accomplished, and scores achieved where applicable.

(2) Records of training provided to individuals shall be retained in electronic or hard copy form. Records shall be retained according to guidance provided in DOE 1324.5B, RECORDS MANAGEMENT PROGRAM, of 1-12-95, and General Records Schedules issued by the Archivist of the United States.

(a) Records of training provided at the Central Training Academy shall be maintained at the Academy and shall also be maintained by the organization sponsoring the individual.

(b) Records of training provided at DOE Elements shall be maintained at DOE Headquarters or the relevant Operations Office, as appropriate, and shall be provided to the organization sponsoring the individual for inclusion in the individual's record file.

(c) Records of training provided at contractor facilities shall be provided to and retained by the organization sponsoring the individual.

(d) Records of training provided at other government or private facilities shall be obtained and maintained by the organization sponsoring the individual.

4. CONTACT. Comments and inquiries on this chapter may be directed to the Materials Control and Accountability Program Manager at (301) 903-2536.

CHAPTER III

PERFORMANCE ASSURANCE PROGRAM

1. OBJECTIVE. To demonstrate the effectiveness of the protection posture for Category I and Category II quantities that roll up to the Category I category of special nuclear material and Top Secret matter by systematically evaluating systems that provide essential protection measures.

2. APPLICABILITY. The program applies to safeguards and security systems and their essential components (e.g., equipment, hardware, administrative procedures, protective forces, personnel) that are used to protect Category I and II special nuclear materials and/or Top Secret matter.

3. PROGRAM REQUIREMENTS. Performance assurance shall be provided for systems and/or system components for those systems providing essential protection for Category I and Category II special nuclear material and/or Top Secret matter.

   a. Performance assurance programs shall provide for operability and effectiveness tests of systems and/or components of systems. Systems and/or essential components of systems whose failure would reduce protection to an unacceptable level shall be tested at a frequency that provides high assurance of reliability for those systems and/or components. Testing frequencies shall reflect site-specific conditions, operational needs, and threat levels. Testing frequencies shall be documented.

      (1) Operability tests provide a simple measure of integrity on a frequent basis. Operability testing shall consist of checking the system element or total system to confirm, without any indication of effectiveness, that it is operating.

      (2) Effectiveness tests provide comprehensive assurance of integrity on an infrequent basis. Performance testing of equipment for effectiveness shall consist of checking systems to confirm the satisfactory performance of the required functions over the expected range of use.

   b. The adequacy of new and existing protective systems shall be confirmed through testing prior to operational use and periodically thereafter.

   c. At least every 365 days, a performance test encompassing protection systems associated with a comprehensive site or facility threat scenario shall be conducted to demonstrate overall facility safeguards and security system effectiveness.

4. DOCUMENTATION REQUIREMENTS.

   a. Performance Assurance Program Plan. This plan may be an integral part of the Site Safeguards and Security Plan or other security plan, as applicable. The plan shall describe the program and its administration and implementation by:

(1) identifying protection elements for the protection of Category I and II special nuclear material and Top Secret matter;

(2) describing how the performance of these elements is to be ensured, including the manner in which activities performed by external oversight organizations will be applied and interpreted; and

(3) addressing unsatisfactory results of performance assurance activities, how they are to be captured in the site corrective action program, and how corrections will be implemented.

b. Performance Assurance Reports. Performance Assurance Reports shall be prepared to document results of implementation of performance assurance activities.

c. Document Retention.

(1) Recordkeeping systems shall provide an audit trail for performance assurance activities and reports.

(2) Disposition of documents shall be in accordance with DOE 1324.5B, RECORDS MANAGEMENT PROGRAM, of 1-12-95.

5. CONTACT. Comments and inquiries on this chapter may be directed to the Protection Operations Program Manager at (301) 903-4244.

CHAPTER IV

SAFEGUARDS AND SECURITY AWARENESS PROGRAM

1. OBJECTIVES.

   a. As a condition for access to classified information, special nuclear materials, and/or unescorted access to DOE Security Areas, excepting Property Protection Areas, individuals shall receive briefing(s). In addition, as a condition for access to classified information, individuals shall execute the Classified Information Nondisclosure Agreement.

   b. Individuals shall be precluded or restricted from unescorted access to such DOE Security Areas and/or from access to classified information or special nuclear materials until the requirements of this chapter have been satisfied.

2. APPLICABILITY. A safeguards and security awareness program shall be developed, implemented, and maintained at each DOE and covered contractor site/facility having such DOE Security Areas, classified matter, and/or special nuclear materials.

3. PROGRAM REQUIREMENTS.

   a. Safeguards and Security Awareness Coordinator. Each affected DOE Element shall appoint a Safeguards and Security Awareness Coordinator who shall ensure that the requirements of this Chapter are met.

   b. Classified Information Nondisclosure Agreement. Prior to being granted access to classified information, individuals granted DOE access authorizations shall execute a Classified Information Nondisclosure Agreement. A refusal to execute the Classified Information Nondisclosure Agreement shall be grounds for the denial to classified information.

   c. Briefings. Safeguards and security awareness programs shall include, but are not limited to, the development and presentation of four briefings:

      (1) Initial Briefing.

      (2) Comprehensive Briefing.

      (3) Refresher Briefing.

      (4) Termination Briefing.

Vertical line denotes change.

d. Topics. Safeguards and security awareness programs shall incorporate the dissemination of information concerning the following:

(1) Applicable DOE safeguards and security, directives and procedures.

(2) Site-specific (and/or operations-specific) safeguards and security policies, procedures, and requirements.

(3) Other matters of safeguards and security interest, such as:

(a) recent espionage cases,

(b) approaches and recruitment techniques employed by foreign intelligence services,

(c) safeguards or security incidents and considerations, and

(d) safeguards or security threats and vulnerabilities.

c. Initial Briefing.

(1) Individuals approved for unescorted access to Security Areas (except Property Protection Areas) shall receive an Initial Briefing.

(2) Briefing topics shall include, but are not limited to:

(a) overview of DOE safeguards and security disciplines, to include personnel security, information security, and physical security;

(b) local access control procedures and escort requirements;

(c) protection of Government property;

(d) prohibited articles; and

(e) reporting of incidents of safeguards and security concern.

d. Comprehensive Briefing.

(1) Prior to being granted access to classified information or special nuclear materials, individuals granted DOE access authorizations shall receive a comprehensive briefing to inform them of their safeguards and security responsibilities. When such individuals are assigned to another DOE site, they shall receive comprehensive briefings at the new site.

Vertical line denotes change.

(2) Briefing topics shall include, but are not limited to, the following:

(a) Information Security.
(b) Physical Security.
(c) Personnel Security.
(d) Reporting/notification requirements.
(e) Legal and administrative sanctions imposed for incurring a security infraction or committing a violation.
(f) General information concerning the protection of special nuclear materials.

g. Refresher Briefings. Individuals who possess DOE access authorizations shall receive refresher briefings to reinforce and update awareness of safeguards and security policies and their responsibilities. Refresher briefings are mandatory for all individuals possessing DOE access authorizations and shall be implemented each calendar year at approximately 12-month intervals.

h. Termination Briefings. Individuals shall receive termination briefings to inform them of their continuing security responsibilities after their access authorizations are terminated. A termination briefing shall be implemented on the individual's last day of employment, the last day the individual possesses an access authorization, or the day it becomes known that the individual no longer requires access to classified information or special nuclear materials, whichever is sooner. Termination briefings shall be based on the information contained in DOE F 5631.29, "Security Termination Statement," and the Classified Information Nondisclosure Agreement.

i. Manual. A Manual for this program shall be developed and maintained by the Office of Safeguards and Security for distribution to DOE Elements and covered contractors having DOE Security Areas, classified matter, and/or special nuclear materials to facilitate the implementation of this chapter.

4. DOCUMENTATION REQUIREMENTS.

a. Recordkeeping. Records shall be maintained to identify all individuals who have received briefings by type and date of briefing. Recordkeeping systems shall be capable of providing an audit trail.
b. Documentation.
(1) A completed Classified Information Nondisclosure Agreement may serve as documentation for the Comprehensive Briefing.
(2) In recurring requirements, such as the refresher briefing, records shall be maintained until the next occurrence of the briefing.
(3) The completion of DOE F 5631.29 satisfies documentation requirements for the termination briefing.

5. CONTACT. Comments and inquiries on this chapter may be directed to the Personnel Security Program Manager at (301) 903-3602.

Vertical line denotes change.

CHAPTER V

FACILITY CLEARANCES AND REGISTRATION OF SAFEGUARDS AND SECURITY ACTIVITIES

1. OBJECTIVES. To ensure proper levels of protection consistent with Departmental standards to prevent unacceptable, adverse impact on national security or on the health and safety of DOE and contractor employees, the public, or the environment are afforded safeguards and security activities.

2. APPLICABILITY. This chapter applies to DOE Elements and personnel performing safeguards and security tasks and responsibilities addressed in this chapter and in other Safeguards and Security directives.

3. REQUIREMENTS: GENERAL.

   a. Nuclear and other hazardous materials presenting a potential radiological or toxicological sabotage threat, classified matter, and property protection interests shall not be permitted on premises occupied by the Department or its contractors until facility clearance is granted.

   b. Safeguards and security activities involving access authorizations shall be registered to assist in ensuring proper levels of protection consistent with Departmental standards to prevent unacceptable, adverse impact on national security or on the health and safety of DOE and contractor employees, the public, or the environment.

   c. If no need exists for a contractor's office locations to receive, process, reproduce, store, transmit, or handle classified information or nuclear material, but access authorizations are required for the contractor to perform the work within DOE-approved facilities, the contractor (identified as a non-possessing facility) must be cleared. As used in this Order, the term facility clearance refers to both possessing and non-possessing facilities.

   d. Facility clearance shall be based upon a determination that satisfactory safeguards and security measures can be afforded the safeguards and security activities. The determination of a valid facility clearance shall be based upon an approved safeguards and security plan, results of surveys, and a favorable FOCI determination, as appropriate.

   e. Approval for other Federal agency safeguards and security activities to be conducted at Department-owned or -operated facilities shall be based upon a determination that the safeguards and security measures to be provided are consistent with Departmental policy. Before acceptance of non-DOE safeguards and security activities, the Department and the requesting agency shall exchange appropriate classification and protection information. The exchange shall be documented in an agreement, which shall include appropriate reimbursement for safeguards and security costs incurred by the Department.

f. Facility clearance for work for others safeguards and security activities at other than Department-owned or -operated facilities that are channeled through a Departmental entity shall be based upon validation of the other agency's facility clearance.

(1) Before commencement of non-DOE funded work, conduct, as required by DOE 5650.2B, IDENTIFICATION OF CLASSIFIED INFORMATION, a review of the work request and certify that the sponsoring organization has either provided the appropriate classification guidance or has stated in writing that the non-DOE funded work will not entail classified activities.

(2) Ensure, prior to commencement of the non-DOE funded work involving access authorizations, that safeguards and security activities have been recorded as security interests on DOE F 5634.2 or DD F 254, "Contract Security Classification Specification."

(3) Ensure, before acceptance of any work for another Federal agency, that appropriate reimbursement for safeguards and security costs is negotiated.

4. REQUIREMENTS: LEAD RESPONSIBLE OFFICE.

a. The Lead Responsible Office grants facility clearance for eligible facilities under its cognizance.

b. If more than one Departmental Element has a registered activity at a facility, the organization responsible for the activity involving the highest classification level and category of activity is normally the Lead Responsible Office. However, this responsibility may, by mutual agreement, be accepted by a Responsible Office that does not have the highest classification level and category of activity, but has a greater scope of activity, such as with long term or traditional interests.

c. Any change in the Lead Responsible Office must include a transfer of appropriate documentation (e.g., safeguards and security plans, FOCI case files, status of unresolved findings).

d. Ensure safeguards and security surveys are accomplished using either internal assets or through a Memorandum of Understanding with another Surveying Office.

5. REQUIREMENTS: SAFEGUARDS AND SECURITY INFORMATION MANAGEMENT SYSTEM. Surveying and Lead Responsible Offices shall maintain information in the Safeguards and Security Information Management System for facilities over which they have responsibility, survey cognizance, or registered safeguards and security activities.

a. The Safeguards and Security Information Management System shall reflect facility information, activity information, and survey information.

b. Changes shall be accurately recorded and coordinated with the Lead Responsible Office in a timely manner.

c. Lead Responsible and Surveying Offices shall ensure that the Safeguards and Security Information Management System maintained at the Office of Safeguards and Security reflects established facilities and safeguards and security activities, under their jurisdiction, via prompt submission of accurate DOE F 5634.3 and DOE F 5634.2 and shall periodically review the Safeguards and Security Information Management System database to confirm the information contained therein is accurate.

6. REQUIREMENTS: FACILITY CLEARANCES. Facility clearances are recorded by Lead Responsible Offices, on DOE F 5634.3, "Facility Data and Approval Record" (see paragraph 7 of this chapter).

a. Granting Approval. Approval of a facility is based on the following:

(1) A favorable foreign ownership, control, or influence determination, in accordance with Chapter VI.

(2) A Facility National Agency Check, which has been requested or completed on those facilities that do not possess a Department of Defense (DOD) facility clearance, in accordance with Chapter VI.

(3) For contractors, contract(s) containing appropriate security clauses.

(4) Approved safeguards and security plans, as appropriate.

(5) If nuclear materials are involved, an established Reporting Identification Symbol code for Nuclear Materials Management and Safeguards System reporting.

(6) For the facility to possess classified matter, nuclear and other hazardous material presenting a potential radiological or toxicological sabotage threat, or over $5,000,000 of DOE property, not including facilities or land values, at its location, an initial survey or other survey resulting in a report that comprehensively addresses the security interest, conducted no more than 6 months before the facility clearance date, with a composite facility rating of satisfactory.

(7) Appointment of a Facility Security Officer and, if applicable, Materials Control and Accountability Representative. The Facility Security Officer must possess a access authorization equivalent with the facility clearance.

(8) Access authorizations for appropriate personnel. Key management personnel must be determined case by case. The Lead Responsible Office FOCI Operations Manager, in conjunction with the Facility Clearance Operations Manager, is responsible for determining

an organization's key management personnel. Key management personnel must possess access authorizations equivalent with the level of the facility clearance. Other officials, to be determined by the Lead Responsible Office, must possess appropriate access authorization for classified information or special nuclear materials.

b. Accepting a Contractor's Existing Federal Agency Facility Clearance. A contractor holding facility clearance from another Federal agency may be approved by DOE for processing, using, or storing classified matter, contingent on the following.

(1) The Federal agency facility clearance is at the appropriate classification level and encompasses the DOE activity. The other Federal agency's facility clearance shall not be accepted if it is based on a Special Security Agreement, Security Control Agreement, Limited Facility Clearance, or Reciprocal Clearance.

(2) The cognizant Federal agency agrees that it shall not cancel the facility clearance without prior notification to the Lead Responsible Office.

(3) The last survey report is acceptable in those areas that could affect the DOE activity.

(4) The cognizant Federal agency agrees to furnish the Lead Responsible Office copies of its periodic survey reports or memoranda covering the DOE activity.

(5) Each employee to be granted access to DOE classified information has, as a minimum, a Federal security clearance equivalent to that required by DOE, or reconciliation through interagency coordination on a case-by-case basis.

(6) If Restricted Data (RD) or Formerly Restricted Data (FRD) are involved, the cognizant Federal agency has provided assurance of compliance with the requirements of the Atomic Energy Act of 1954, as amended, including the mandatory personnel clearance requirements.

(7) The requirements identified above have been documented in a letter or memorandum of agreement between the Lead Responsible Office and the cognizant Federal agency.

c. Verification of Federal Agencies. Verification of the capability of another Federal agency is based on written assurance from that agency that:

(1) classified matter shall be afforded protection according to Executive Order 12958, "National Security Information," and its implementing Information Security Oversight Office directives; and

(2) the requirements of the Atomic Energy Act of 1954, as amended, pertaining to access to Restricted Data and Formerly Restricted Data, including the mandatory personnel clearance requirements, shall be met.

When Restricted Data or Formerly Restricted Data is involved, this written assurance shall include coordination and reconciliation procedures to limit the manner in which this data is to be disseminated.

d. Suspension of Facility Clearance. The facility clearance for a contractor determined to be under FOCI shall be suspended pending final resolution and implementation of the security measures required to negate or reduce the foreign involvement. The contractor shall also be advised that failure to adopt required security deemed appropriate pending final resolution, may result in termination of its facility clearance. When findings or other deficiencies indicate suspension of a facility clearance is necessary, the responsible Head of Departmental Element, in coordination with the Office of Safeguards and Security, as appropriate, may suspend the facility clearance pending validated corrective actions. Once a decision is made to suspend the facility clearance, all affected Departmental Elements shall be notified by the Lead Responsible Office. The contractor subject to suspension action shall be notified that its facility clearance has been suspended, that performance on existing classified contracts may continue unless notified by DOE to the contrary, and that the award of new classified contracts will not be permitted until that facility clearance has been restored to a fully valid status.

e. Reinstatement. Following a survey to validate that corrective actions have been accomplished that restore a facility's safeguards and security posture to a composite satisfactory facility rating, the facility clearance may be reinstated. The Lead Responsible Office must complete a DOE F 5634.3 to enact the reinstatement.

f. Terminating Approval. When a facility has completed all safeguards and security activities involving work requiring access authorizations, nuclear and other hazardous material presenting a potential radiological or toxicological sabotage threat, classified matter, or over $5,000,000, exclusive of facility and land values) of Departmental property, the Lead Responsible Office shall ensure (1) a termination survey, as identified in Chapter IX, is conducted to verify appropriate disposition, destruction, or return of classified matter, nuclear and other hazardous material presenting a potential radiological or toxicological sabotage threat, or Departmental property to DOE custody and (2) termination of all affected access authorizations. The Lead Responsible Office shall then terminate the facility clearance.

When a facility has been determined to have significant unresolved deficiencies or is under FOCI, the primary consideration shall be the safeguarding of classified information and/or special nuclear material. The Lead Responsible Office is responsible for taking whatever interim action it believes necessary to safeguard classified information and/or special nuclear material, in coordination with other affected DOE offices as appropriate. If the facility does not have possession of classified information and/or special nuclear material, and does not have a current or impending requirement for such access, the facility clearance shall be terminated. If final agreement by the parties with regard to the security measures to resolve deficiencies or to negate or reduce the foreign involvement to an acceptable level, as determined by DOE, are not attained within a prescribed period of time, the facility clearance shall be terminated.

7. REQUIREMENTS: FACILITY DATA AND APPROVAL RECORD.

a. Purpose. The Facility Data and Approval Record is used to register pertinent facility information on the Safeguards and Security Information Management System. The Lead Responsible Office shall record a single DOE F 5634.3 to reflect the highest approved safeguards and security activity. Prompt entry on the Safeguards and Security Information Management System and accuracy of reported information are essential to the continued integrity of the safeguards and security program.

b. Preparation. A DOE F 5634.3 shall be prepared by the procurement request originator, who forwards the completed form to the cognizant Departmental safeguards and security organization. Upon receipt, the responsible Operations Office safeguards and security organization or the Office of Safeguards and Security shall evaluate, survey, and approve the facility based upon an approved safeguards and security plan, safeguards and security surveys with a composite rating of satisfactory, and, if appropriate, a favorable FOCI determination.

(1) If a subcontract is established between a DOE prime contractor and another contractor for work involving access authorizations, classified matter, or nuclear and other hazardous material presenting a potential radiological or toxicological sabotage threat, it is the responsibility of the prime contractor to ensure proper preparation of a DOE F 5634.3.

(2) The Contracting Officer's Representative shall be responsible for validating information on the initial and subsequent DOE F 5634.3 and forwarding the form to the responsible DOE safeguards and security organization for approval.

c. Approval. DOE F 5634.3 shall be approved by the Lead Responsible Office.

d. Registration. The DOE F 5634.3, "Facility Data and Approval Record," must be completed by the Lead Responsible Office in order to register:

(1) facility clearance;

(2) a significant change in a facility (e.g., a change in name, address, Lead Responsible Office, classified mailing/shipping address, nuclear materials categorization, or classification level and category of information authorized);

(3) facility clearance termination;

(4) suspension of a facility clearance; or

(5) reinstatement of a suspended facility clearance.

e. Attachments. A copy of the facility's safeguards and security plan(s), survey report(s), and pertinent correspondence shall be maintained with DOE F 5634.3 for facility clearance. For facility termination a copy of the certificate of non-possession must be maintained.

8. REQUIREMENTS: ACTIVITY REGISTRATION. Activity registration is recorded on DOE F 5634.2, "Contract Security Classification Specification." (See paragraph 9 of this chapter.)

a. Accepting Existing DOE Facility Clearance.

(1) A Departmental Element seeking to establish an activity shall check the Safeguards and Security Information Management System to determine whether the contractor or prospective contractor currently holds a facility clearance. In coordination with the Lead Responsible Office, an organization may accept the existing facility clearance, provided:

(a) the new activity shall be protected adequately under the facility's existing safeguards and security program as outlined in the applicable, approved safeguards and security plan;

(b) the existing facility clearance is compatible with the level of the new activity; and

(c) the facility holds a composite facility rating of satisfactory on the basis of the last safeguards and security survey report.

(2) When an activity will exceed the current facility clearance or a facility clearance does not exist, the actions required in paragraph 6 must be completed, as appropriate. The upgrading of a facility clearance may also require the transfer of the functions of the Lead Responsible Office.

b. Suspension of an Activity at a Facility. When current deficiencies indicate to responsible management officials that suspension is necessary for a specific activity, the Departmental Element establishing an activity, in coordination with the Lead Responsible Office, may suspend the activity and the ability of the facility to accept new safeguards and security activities pending correction of those deficiencies and validation of those corrective actions.

c. Reinstatement. Upon completion of a survey that validates corrective actions, the suspended activity may be reinstated. A DOE F 5634.2 is required to enact the reinstatement.

d. Terminating an Activity at a Facility. When a registered activity is terminated at an approved facility, the organization that established the activity must ensure that all affected access authorizations are terminated, and all nuclear and other hazardous material presenting a potential radiological or toxicological sabotage threat, DOE property, and/or classified matter is appropriately reallocated, disposed of, destroyed, or returned to an appropriate organization. A certificate of non-possession shall be obtained from the Lead Responsible Office and maintained by the organization that established the activity.

9. REQUIREMENTS: CONTRACT SECURITY CLASSIFICATION SPECIFICATION.

   a. New Activity. If a new activity for work involving access authorizations is being considered, the DOE F 5634.2 (or the DD F 254, Contract Security Classification Specification) must be submitted by the procurement request originator, to the Contracting Officer's Representative. These forms are used to register pertinent activity information on the Safeguards and Security Information Management System. The Contracting Officer's Representative shall validate the information on the DOE F 5634.2 (or DD F 254) and forward the form to the responsible DOE safeguards and security organization for approval.

   b. Preparation. A DOE F 5634.2 shall be initially prepared by the procurement request originator, who forwards the completed form to the cognizant Departmental Element Safeguards and Security organization. If a DD F 254, "Contract Security Classification Specification," has been used by the agency sponsoring the activity, it shall be annotated with the facility code and submitted instead of the DOE F 5634.2.

10. REQUIREMENTS: FACILITY IMPORTANCE RATINGS. Importance ratings shall be used to identify relative importance of facilities on the Safeguards and Security Information Management System and to determine survey frequency. A detailed explanation of these ratings is located in the Safeguards and Security Survey and Self-Assessment Guide.

11. IMPLEMENTATION ASSISTANCE. The Office of Safeguards and Security will develop an implementation plan for the implementation of DOE F 5634.2 and DOE F 5634.3 in the Safeguards and Security Information Management System. This implementation plan will be provided to each Lead Responsible Office and Survey Office, who shall use this plan to develop a local implementation plan.

12. CONTACT. Comments and inquiries regarding this chapter may be directed to the Technical and Operations Security Program Manager at (301) 903-5217.

CHAPTER VI

FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE PROGRAM

1. OBJECTIVE. It is DOE policy to obtain information that indicates whether offerors/bidders or contractors are owned, controlled, or influenced by a foreign person and whether as a result the potential for an undue risk to the common defense and national security may exist.

2. APPLICABILITY. Foreign ownership, control, or influence (FOCI) determinations are required of the following.

   a. Contractors, which include any industrial, educational, commercial, or other entity, grantee, or licensee, including an individual, that has executed an agreement with the Federal Government for the purpose of performing under a contract, license, or other arrangement that requires access authorizations. However, the foregoing does not include individuals performing work under a consulting agreement. This includes subcontractors of any tier, consultants, agents, grantees, and cooperative agreement participants.

   b. All tier parents, if the contractor is owned or controlled by another firm(s).

3. REQUIREMENTS.

   a. A favorable FOCI determination must be rendered on the prospective contractor and, if applicable, its tier parents, prior to the Lead Responsible Office granting a facility clearance or contract requiring access authorizations. Unless established thresholds are exceeded, the Lead Responsible Office shall render the FOCI determination(s) on the contractor and, if applicable, tier parents.

   b. While the Lead Responsible Office will conduct a preliminary review of the FOCI representations and certifications of each firm in the competition range in a procurement request, a facility clearance, which requires a FOCI determination, can only be requested for the successful offeror/bidder if there is expected to be insufficient lead time between selection and contract award to allow deferral of the FOCI determination and facility registration.

   c. Prior to the award of a contract requiring access authorizations to an offeror/bidder that does not possess a facility clearance, the offeror/bidder shall be required to submit to the Contracting Officer information and documentation that define the extent and nature of any foreign ownership, control, or influence over the offeror/bidder and, if applicable, its tier parents. The Contracting Officer cannot award the contract/agreement until he/she receives notification from the Lead Responsible Office that a favorable FOCI determination was rendered.

d. A contractor with a facility clearance is required to ensure that the following notification for its organization and each of its tier parents is immediately provided to the Lead Responsible Office.

(1) Written notification of a change in the extent and nature of FOCI that affects the information in the FOCI representation and certification .

(2) Complete, current, and accurate information, certifications, and explanatory documentation that define the extent and nature of any relevant FOCI whenever:

(a) there is any change in ownership or control;

(b) 5 years have elapsed since the previously provided FOCI representations and certification were executed; or

(c) the Lead Responsible Office advises that it considers that a relevant change in the nature of the FOCI has occurred.

(3) Written notification of anticipated changes that include, but are not limited to, the following:

(a) action to terminate the contractor organization or any of its parents for any reason;

(b) imminent adjudication of or reorganization in bankruptcy of the contractor organization or any tier parents;

(c) discussions or consultations with foreign interests that may reasonably be expected to lead to the introduction or increase of FOCI; or

(d) negotiations for the sale of securities to a foreign interest that may lead to the introduction or increase of FOCI.

e. Contracting Officers must provide written notification to the servicing safeguards and security office in each of the following instances:

(1) A FOCI determination is required on an offeror/bidder and, if applicable, its tier parents. The Contracting Officers will send the servicing safeguards and security office the FOCI representations and certifications and supporting documentation, which have been reviewed for completeness.

(2) A requested FOCI review is no longer needed.

(3) A FOCI determination was rendered on an offeror/bidder that was not the successful bidder.

(4) Within 30 days of the termination or completion of all work by the contractor on a contract requiring access authorizations.

f. The Lead Responsible Office shall provide the successful offeror/bidder with written notification that:

(1) DOE has reviewed the FOCI submission and determined the organization is not under FOCI; or

(2) the contractor and any tier parents must keep the FOCI information current;

(3) identifies the Lead Responsible Office. This office is the only office to which the contractor and any tier parents will provide new FOCI representation and certification or written notification of anticipated or significant changes.

g. When established thresholds are exceeded, the Office of Safeguards and Security reviews FOCI cases submitted by a Lead Responsible Office to determine eligibility for a FOCI determination.

h. When a tier parent has not entered into a contract requiring access authorizations or is performing work on a contract requiring a lower level access authorization, the Lead Responsible Office shall obtain appropriate Board Resolutions from the contractor and its parent organization(s) to exclude the parent organization(s) from having any unauthorized access.

i. If a contractor, offeror/bidder, and/or tier parent is determined to be under FOCI, the Lead Responsible Office shall ensure that the contractor is advised of the existence of FOCI and the security measures, if any that would be necessary to negate or reduce that foreign involvement and its effect.

j. When the offeror or bidder requiring access authorizations is a local, State, or Federal governmental agency or department, the affected contract must contain a security clause stating that if the governmental agency or department subcontracts any work requiring access authorizations to a commercial entity, their acquisition regulation, including FOCI policies will be followed. In the absence of their own FOCI policies, the DOE will render the FOCI determination.

k. To the extent permitted by law, information submitted in confidence as business/financial information shall be protected as Official Use Only, exempt from public release under the Freedom of Information Act.

4. ELIGIBILITY REQUIREMENTS. An organization will be considered under FOCI when a foreign person has the power, direct or indirect, whether or not exercised, and whether or not exercisable through ownership of the organization's and/or it tier parents' securities, through indebtedness, by contractual arrangements, or other means, to direct or decide matters affecting the

management or operations of that organization in a manner that may result in the compromise of classified information or unauthorized access to nuclear and other hazardous material presenting a potential radiological or toxicological sabotage threat or that may adversely affect the performance of contracts requiring access authorizations. Eligibility requirements include, but are not limited to, the following.

a. A organization effectively owned or controlled by a foreign government is ineligible for award of a contract if it is necessary for the organization to be given access to information in a proscribed category in order to perform the contract unless the foreign government ownership occurred prior to October 23, 1992. The Secretary of Energy may determine that a waiver from this requirement is essential to the national security interest of the U.S.

b. A organization that is owned, controlled, or influenced by a foreign person from a sensitive country identified in DOE 1500.3, FOREIGN TRAVEL AUTHORIZATION, of 11-10-86, and DOE 1240.2B, UNCLASSIFIED VISITS AND ASSIGNMENTS BY FOREIGN NATIONALS, of 8-21-92 shall not be eligible, in some cases, for a favorable FOCI determination. The Office of Safeguards and Security will make the determination.

c. An organization that is owned, controlled, or influenced by a foreign person from a nonsensitive country shall be eligible for a favorable FOCI determination provided action can be taken to effectively negate or reduce associated FOCI risk to an acceptable level. The Office of Safeguards and Security will make the determination.

d. Key management personnel determined to require access authorizations, as set forth in Chapter V, paragraph 6a(8) must possess an access authorization to the level of the facility clearance.

5. REQUIREMENTS: PROCESSING CONTRACTORS FOR FOCI DETERMINATIONS.

a. The Contracting Officer will verify whether the offeror/bidder has a facility clearance through the Safeguards and Security Information Management System. If an offeror/bidder does not possess a facility clearance, the DOE contracting office shall request a complete FOCI package from the organization, and all tier parents. If the parent(s) has a facility clearance, a new FOCI package is not necessary. This package is reviewed for completeness by the DOE Contracting Officer and submitted to the servicing safeguards and security office.

b. Prior to a FOCI determination being rendered, the Lead Responsible Office must accomplish the following.

(1) Receive written confirmation of a contractor's facility clearance from the Defense Investigative Service (DIS)/Central Verification Activity (CVA). When the contractor has a Limited Facility Clearance (formerly "Reciprocal" clearance) or DIS/CVA cannot verify the contractor's clearance and provides a telephone number to call for verification, the FOCI submission must be immediately forwarded to the Office of Safeguards and Security for adjudication; or

(2) Request the Office of Safeguards and Security to obtain a Facility National Agency Check (FNAC) if the contractor does not have an active DOE or DOD facility clearance requiring access authorizations. However, the Lead Responsible Office can render the FOCI determination pending the results of the FNAC, under the following conditions.

(a) The responses to the FOCI questions do not exceed the thresholds established by the Office of Safeguards and Security.

(b) Exclusion procedures are invoked when the contractor requiring access authorizations is controlled by a parent(s) either not requiring access authorizations or requiring a lower-level access authorization.

(3) If the FOCI case exceeds established thresholds, the Lead Responsible Office shall forward the case file to the Office of Safeguards and Security with a recommended determination. Forwarded case files shall contain certifications from the offeror/bidder/contractor and any tier parents and shall document the reasons the case has been forwarded. The Office of Safeguards and Security shall review the package to determine if it concurs with the Lead Responsible Office's recommendation. The Office of Safeguards and Security, in coordination with General Counsel when appropriate, shall provide a final FOCI determination to the Lead Responsible Office.

6. REQUIREMENT: ACCEPTING A FOCI DETERMINATION RENDERED BY ANOTHER FEDERAL AGENCY. DOE will accept another Federal agency's FOCI determination when the requirements for accepting a facility clearance in Chapter V, paragraph 6b, are met.

7. REQUIREMENT: SCHEDULE OF REQUIREMENTS FOR PROCESSING FOCI DETERMINATIONS.

a. The Lead Responsible Office shall observe the following schedule in processing FOCI determinations.

(1) Initial review and verification procedures shall be accomplished within 15 working days of the receipt of a FOCI submission from the contracting officer.

(2) Within an additional 20 working days, one of the following actions will be taken.

(a) A FOCI determination will be rendered by the Lead Responsible Office if FOCI thresholds are not exceeded.

(b) If required, additional information, shall be requested either verbally or in writing from the offeror/bidder/contractor.

(c) The FOCI case, which has been reviewed for completeness, shall be forwarded to the Office of Safeguards and Security if established thresholds are exceeded.

b. For cases forwarded to the Office of Safeguards and Security for action, the foregoing schedule shall also be observed.

c. If for any reason a FOCI determination has not been rendered within 90 working days of receipt:

(1) The Lead Responsible Office shall either (i) provide written notification to the submitting contracting officer with a copy to the Office of Safeguards and Security regarding the reason for the delay in processing/completing the submission or (ii) return the submission to the submitting contracting officer if the contractor has been non-responsive to the Lead Responsible Office's request for additional information or implementation or required security measures.

(2) The Office of Safeguards and Security shall either (i) provide written notification to the Lead Responsible Office regarding the reason for the delay in processing/completing the submission or (ii) return the submission to the Lead Responsible Office if the contractor has been non-responsive to the Office of Safeguards and Security's request for additional information or implementation of required security measures.

8. REQUIREMENTS: SIGNIFICANT CHANGES. When changes in the extent and nature of FOCI that would affect the information in a contractor's and/or any tier parents' most recent DOE FOCI submission(s) have occurred, the contractor/parent shall immediately provide written notification and supporting documentation relevant to the changes to the DOE Lead Responsible Office. A significant FOCI increase/change that warrants processing of the contractor/parent for a new FOCI determination includes, but is not necessarily limited to, the following.

a. A new threshold or factor that did not exist when the previous determination was made (e.g., a "no" answer changes to a "yes" answer), and any additional factors associated with the questions on the FOCI representation and certification.

b. A previously reported threshold or factor that was favorably evaluated by the Lead Responsible Office has increased to a level requiring a determination by the Office of Safeguards and Security.

c. A previously reported financial threshold or factor that was favorably evaluated has increased by 5 percent or more; or a shift has occurred of 5 percent or more by country location of end user (i.e., for revenue and/or net income) or lenders (i.e., indebtedness).

d. A previously reported foreign ownership threshold or factor that was favorably evaluated by the Office of Safeguards and Security has increased to the extent that a method of negation or reduction (see paragraphs 10 and 11) is necessary.

e. Any changes in the ownership or control of the contractor and/or any tier parents.

9. REQUIREMENTS: ADVERSE DETERMINATION. When an offeror/bidder or contractor determined to be under FOCI will not implement the necessary security measures, as determined by DOE, to negate or reduce foreign involvement to an acceptable level, an adverse determination will be rendered by the Office of Safeguards and Security. When a contractor with a FOCI determination experiences significant changes in its FOCI resulting in a determination that the contractor is under FOCI, the contractor's facility clearance shall be suspended and may be terminated, as set forth in Chapter V, paragraphs 6d to f.

10. REQUIREMENTS: METHODS TO NEGATE OR REDUCE UNACCEPTABLE FOCI. The affected U.S. organization(s), or its legal representatives may propose a plan to negate or reduce unacceptable FOCI; however, DOE reserves the right and has the obligation to impose any security method, safeguard, or restriction it believes necessary to ensure that unauthorized access to classified information and/or special nuclear materials is precluded. A plan may consist of one or more of the insulating measures prescribed in paragraph 11 as appropriate. It may also consist of other measures employed in conjunction with, or apart from, these methods, such as:

a. physical or organizational separation of the component performing the work requiring access authorizations,

b. modification or termination of agreements with foreign persons,

c. diversification or reduction of agreements with foreign persons,

d. diversification or reduction of revenue from foreign persons,

e. assignment of specific security duties and responsibilities to selected officials of the organization,

f. creation of special executive-level committees to consider and oversee classified information and/or special nuclear material.

11. REQUIREMENTS: METHODS TO NEGATE OR REDUCE RISK IN FOREIGN OWNERSHIP CASES.

a. National Interest Determination. An organization cleared under a Special Security Agreement and its cleared employees may only be afforded access to "proscribed information" with special authorization. This special authorization must be manifested by a favorable national interest determination that must be program/project/contract-specific. Access to proscribed information must be predicated on compelling evidence that release of such information to an organization cleared under the Special Security Agreement arrangement advances the national security interests of the United States. The authority to make this determination shall not be permitted below the Assistant Secretary. In all majority ownership cases, national interest determination will be prepared and sponsored by the Contracting Officer whose contract or program, is involved and it shall include the following information.

(1) Identification of the proposed awardee and a synopsis of its foreign ownership (include solicitation and other reference numbers to identify the action).

(2) General description of the procurement and performance requirements.

(3) Identification of national security interest involved and the ways in which award of the contract helps advance those interests.

(4) The availability of any other U.S. company with the capacity, capability, and technical expertise to satisfy acquisition, technology base, or industrial base requirements and the reasons any such company should be denied the contract.

(5) A description of any alternate means available to satisfy the requirement, and the reasons alternative means are not acceptable.

A national interest determination shall be initiated by the Contracting Officer. A company may assist in the preparation of the determination, but the Contracting Officer is not obligated to pursue the matter unless it believes further consideration to be warranted. The Contracting Officer shall, if it is supportive of the national interest determination, forward the case through appropriate channels. If the proscribed information is under the classification or control jurisdiction of another agency, the approval of the cognizant agency is required (e.g., NSA for COMSEC, DCI for SCI).

It is the responsibility of the cognizant approval authority to ensure that pertinent security, counterintelligence, and acquisitions interests are thoroughly examined.

b. Board Resolution for Noncontrolling Foreign Minority Cases. When a foreign person(s) owns voting stock, directly or indirectly, but is not permitted representation in the U.S. organization (that is, to hold a position as or appoint any of the U.S. organization's management and/or allowed to transfer any of its employees on any of its foreign-owned parent's or other foreign-owned affiliate's employees to the U.S. organization), resolutions by the U.S. organization's board of directors and other actions as described below may be considered to negate or reduce the FOCI.

(1) Resolutions shall address the following.

(a) Acknowledge and describe all FOCI elements; identify foreign persons and describe the type and number of foreign-owned shares.

(b) Acknowledge the organization's obligations to comply with all security program and export control requirements.

(c) Certify that foreign persons shall not require, shall not have, and can be effectively precluded from access to all classified information or nuclear and other hazardous material presenting a potential radiological or toxicological sabotage threat

entrusted to or held by the U.S. organization; certify that the foreign persons will not be permitted representation in the U.S. organization or to influence the organization's policies and practices in the performance of contracts requiring access authorization(s).

(2) Criteria. The following criteria must also be satisfied for a board resolution to serve as the sole method accepted to negate or effectively reduce the risk of compromise arising from foreign ownership within the levels prescribed herein.

(a) Identified U.S. person(s) own a majority of the stock.

(b) A foreign person is not the single largest shareholder.

(3) Publication of the Resolution(s). The U.S. organization shall be required to distribute to its directors and its principal officers copies of such resolutions and report in its corporate records the completion of such distribution. In addition, the substance of the foregoing resolution(s) shall be brought to the attention of all personnel possessing or being processed for an access authorization.

(4) Verification. Compliance with the resolution(s) shall be verified during periodic surveys.

c. Security Control Agreement for Noncontrolling Foreign Minority Cases. When a foreign person(s) owns voting stock, directly or indirectly, and is permitted representation in the U.S. organization (that is, to hold a position as or appoint any of the U.S. organization's management and/or allowed to transfer any of its employees on any of its foreign-owned parent's or other foreign-owned affiliate's employees to the U.S. organization), the Security Control Agreement, as set forth in 11d(4), may be considered to negate or reduce the FOCI.

d. Controlling Foreign Majority Cases. A controlling foreign majority case is one in which foreign person(s) own a majority of the voting securities of the U.S. organization or, if less than 50 percent is foreign-owned, it can be reasonably determined that foreign person(s) or their representatives are in a position to effectively control or dominate the business management of the U.S. organization.

(1) Voting Trust Agreement. A voting trust agreement is an acceptable method to negate or reduce risks associated with a controlling foreign majority case. Under this arrangement, the following requirements must be met.

(a) Foreign stockholders must transfer legal title of foreign-owned stock to the trustees, and the U.S. organization to be cleared must be organized, structured, and financed to operate as a viable business entity independent from the foreign stockholder(s).

(b) The Voting Trust Agreement must unequivocally provide for the exercise of all prerogatives of ownership by the trustees with complete freedom to act

independently and without consultation with, interference by, or influence from foreign stockholders.

(c) There shall be at least three trustees, and all must become members of the U.S. organization's board of directors. In addition, the trustees must:

1 be U.S. citizens residing within the limits of the U.S. and capable of assuming full responsibility for voting the stock and exercising the management prerogatives relating thereto in such a way as to effectively insulate foreign stockholder(s) from the cleared U.S. organization;

2 be completely disinterested individuals with no prior involvement with either the cleared U.S. organization, its foreign-owned tier parent(s), and any of its foreign-owned affiliate(s);

3 be issued and be able to maintain an access authorization to the level of the facility clearance or safeguards and security activity;

4 be approved by the Office of Safeguards and Security when a vacancy occurs due to the resignation or removal of a trustee and a successor trustee is appointed by the remaining trustees;

5 prior to being accepted as trustees by the Office of Safeguards and Security, be advised by the Office of Safeguards and Security of the duties and their responsibilities on behalf of DOE to insulate the cleared U.S. organization from the foreign person(s), and indicate, in writing, their willingness to accept this responsibility.

(d) The voting trust agreement may, however, limit the authority of the trustees by requiring approval from the foreign stockholder(s) with respect to the following.

1 The sale or disposal of the cleared U.S. organization's assets or a substantial part thereof.

2 Pledges, mortgages, or other encumbrances on the capital stock they hold in trust.

3 Corporate mergers, consolidations, or reorganizations.

4 The dissolution of the cleared U.S. organization.

5 The filing of a bankruptcy petition.

(e) Trustees must assume full responsibility for the voting stock and for exercising all management prerogatives relating thereto in such a way as to ensure that the foreign stockholder(s), except for the approvals enumerated above, will be effectively insulated from the cleared U.S. organization and continue solely in the status of beneficiaries.

(f) The Certification and Visitation Approval Procedure Agreement of paragraph 11b(3) is required under this arrangement.

(2) Proxy Agreement. A proxy agreement is an acceptable method to negate or reduce risks associated with controlling foreign majority cases. Under this arrangement, the voting rights of stock owned by foreign persons are conveyed to proxy holders by an irrevocable proxy agreement. Legal title to the stock remains with the foreign persons. All other provisions of the voting trust agreement as they apply to trustees (see paragraph 11b(1)) and the terms of the agreement shall apply to the proxy holders. Conditions for consideration of use of a proxy agreement are the same as required for a voting trust agreement. Proxy agreements must be coordinated with General Counsel.

(3) Visitation Approval Procedure Agreement. In every case where a voting trust agreement or proxy agreement is employed to negate or reduce risks associated with foreign ownership, a visitation approval procedure agreement shall be executed between the cleared U.S. organization, the foreign persons, the Office of Safeguards and Security, and as appropriate, trustees, proxy holders, or other designated individuals. The visitation approval procedure agreement must identify who may visit, for what purposes, when advance approval is necessary, and the approval authority. The cleared U.S. organization shall submit individual requests to the approval authority for each visit. The visitation approval procedure agreement shall provide that, as a general rule, visits between foreign stockholder(s) and the cleared U.S. organization are not authorized; however, as an exception to the general rule, the approval authority may approve such visits in connection with regular day-to-day business operations pertaining strictly to purely commercial products or services and not pertaining to contracts requiring access authorization(s).

(4) Special Security Agreement and Security Control Agreements. The Special Security Agreement and the Security Control Agreements are substantially identical arrangements that impose substantial industrial security and export control measures within an institutionalized set of corporate practices and procedures; require active involvement of senior management and certain Board members in security matters (who must be cleared, U.S. citizens); provide for the establishment of a Government Security Committee to oversee classified and export control matters; and preserve the foreign stockholder's right to be represented on the Board with a direct voice in the business management of the company while denying unauthorized access to classified information.

(a) The Special Security Agreement may be considered to negate or reduce the FOCI for a U.S. organization effectively owned or controlled by a foreign person.

However, access to proscribed information is permitted only with the written permission of the agency with classification or control jurisdiction over the proscribed information (e.g., NSA for COMSEC, DCI for SCI). A determination to disclose proscribed information to a company cleared under a Special Security Agreement requires that a favorable national interest determination be rendered prior to contract award. Additionally, DOE must have entered into a General Security Agreement with the foreign government involved (that is the country to which the foreign ownership stems).

(b) The Security Control Agreement may be considered to negate or reduce the FOCI for an organization not effectively owned or controlled by a foreign person. Limitations on access to classified information are not required under a Security Control Agreement.

12. REQUIREMENTS: ANNUAL REVIEWS AND COMPLIANCE.

a. Annual Review. Representatives of the Lead Responsible Office shall meet annually with senior management officials of organizations operating under a Voting Trust Agreement, Proxy Agreement, Special Security Agreement, or Security Control Agreement to review the effectiveness of the pertinent security arrangement and to establish common understanding of the operating requirements and how they will be implemented within the cleared organization.

b. Annual Certification.

(1) At the end of each year of operation, the trustees, proxy holders, or other principals as appropriate of those organizations operating under a DOE-approved Voting Trust Agreement, Proxy Agreement, Special Security Agreement, or Security Control Agreement shall submit to the Lead Responsible Office an annual implementation and compliance report. Failure of the cleared U.S. organization to ensure compliance with the terms of the applicable security arrangement may result in the organization's facility clearance being suspended pending resolution of the FOCI.

(2) Each contractor holding a facility clearance shall certify annually to the Lead Responsible Office that (i) no significant changes have occurred in the extent and nature of FOCI that would affect the organization's answer to the questions provided in its FOCI representations; (ii) no changes have occurred in the organization's ownership; and (iii) no changes have occurred in the organization's officers, directors, and executive personnel.

(3) When the contractor is controlled by parent organizations that have been excluded, the contractor must also provide annually to the Lead Responsible Office written certification from an authorized official from each such excluded parent that (i) no significant changes have occurred in the extent and nature of FOCI that would affect

the organization's answers to the questions provided in its FOCI representations; (ii) no changes have occurred in the organizations's ownership; and (iii) no changes have occurred in the organization's officers, directors, and executive personnel.

13. CONTACT. Comments and inquiries regarding this chapter may be directed to the Technical and Operations Security Program Manager, telephone (301) 903-5217.

CHAPTER VII

INCIDENTS OF SAFEGUARDS AND SECURITY CONCERN

1. OBJECTIVES.

   a. Programs and procedures shall be established to deter, detect, and ensure the prompt reporting of incidents of safeguards and security concern to DOE.

   b. A systematic inquiry shall be conducted to review the circumstances surrounding an incident of safeguards and security concern to develop all pertinent information and to determine whether an infraction, criminal violation, or loss has occurred. Inquiries shall not be used as a means of holding in abeyance a decision to initiate a full-scale investigation.

2. APPLICABILITY. Incidents of safeguards and security concern are events that, at the time of occurrence, have yet to be determined to be a violation of law, but that are of such concern to the safeguards and security program as to warrant immediate review, inquiry, and subsequent assessment and reporting.

   a. Safeguards and security representatives may conduct preliminary inquiries of incidents of Safeguards and Security concerns, however, they shall not investigate criminal violations except when DOE investigators are deputized agents of State or local law enforcement agencies. Such deputized agents shall consult with the Federal Bureau of Investigation when investigating criminal violations involving DOE and contractor activities, operations, or personnel.

   b. When an inquiry establishes that an alleged or suspected violation of law involving a national security interest has occurred, the appropriate DOE Element shall refer the incident to the Federal Bureau of Investigation and/or the appropriate law enforcement agency.

   c. When an inquiry establishes credible information that fraud, waste and/or abuse has occurred, which does not involve a national security interest has occurred, the Office of the Inspector General shall be notified for information and/or action.

   d. When an inquiry establishes that a potential compromise or unauthorized disclosure of classified information has occurred, the applicable provisions of DOE O 471.2, INFORMATION SECURITY PROGRAM, shall be followed.

   e. Employees with information regarding possible fraud, waste, abuse, or other forms of wrongdoing in the Department's programs or operations shall inform the Inspector General immediately upon obtaining such information.

3. REQUIREMENTS.

a. Safeguards and security directors shall ensure that inquiries are conducted to establish the circumstances surrounding as suspected or alleged criminal violation involving a national security interest or loss involving a national security interest. The authority to conduct such inquiries remains with the Head of the Field Element and, in the case of Headquarters, with the Office of Safeguards and Security.

(1) Inquiry officials (with previous inquiry experience) familiar with appropriate policies and procedures shall be appointed in writing by the Head of the DOE Element. The inquiry official is not authorized to detain individuals for interviews or obtain sworn statements; however, he/she may conduct consensual interviews and obtain signed statements. The inquiry official is responsible for maintaining records of inquiry (e.g., log of events, notes, recordings, statements).

(2) Whenever possible, the responsibility for an incident shall be fixed upon an individual rather than upon a position or office. When individual responsibility cannot be established, and the facts show that a responsible official allowed conditions to exist that led to an incident of safeguards and security concern, responsibility shall be fixed upon such responsible official. Infractions shall be issued in accordance with DOE O 471.2 for a violation of procedures after a determination has been made by the Department of Justice or appropriate authority not to prosecute the violation.

(3) An inquiry shall be instituted within 48 hours from the initial report of the alleged or suspected violation to the Office of Safeguards and Security and cognizant Secretarial Officer.

b. Loss, compromise, or unauthorized disclosure of classified information, and alleged or suspected violations of laws pertaining to safeguards and security shall be reported promptly through the appropriate DOE Element to the Office of Safeguards and Security, the Secretarial Officer, and when appropriate, the local Federal Bureau of Investigation office.

(1) The method and sequence for reporting safeguards and security incidents will depend upon the situation as well as the immediacy of action that may be required to mitigate the situation.

(2) Unclassified reports and notifications of safeguards and security incidents shall be made in accordance with DOE O 232.1 and DOE O 471.2. Reports that contain classified information shall contain all of the information required by DOE O 232.1, but shall not be entered on the Occurrence Reporting and Processing System. Classified reports shall be sent by approved methods for transmitting classified information. Reporting intervals for incidents of safeguards and security concern must be in accordance with DOE O 232.1.

c. Federal Bureau of Investigation personnel shall be admitted to areas and afforded access to Restricted Data or other classified information as necessary for them to perform their duties. Such personnel shall be provided escort, as necessary, for safety reasons or to facilitate the investigative progress.

(1) When Federal Bureau of Investigation personnel are given access to classified information, they will be immediately advised of the classification and the category of the information. Appropriate document and data classification, marking information, and protection and control requirements shall be made available to them through local liaison channels.

(2) The availability of DOE standard security badges and advance notification arrangements shall be determined by agreement between the DOE and Federal Bureau of Investigation organizations involved. This authority does not extend to Sensitive Compartmented Information, which requires special access approval.

4. CONTACT. Comments and inquiries on this chapter may be directed to the Technical and Operations Security Program Manager at (301) 903-5217.

CHAPTER VIII

CONTROL OF CLASSIFIED VISITS PROGRAM

1. OBJECTIVES.

   a. To ensure that only authorized persons with the appropriate access authorization and need-to-know receive access to classified information in connection with visits involving the release or exchange of classified information.

   b. To limit foreign visitor access to classified information to that prescribed in approved Agreements for Cooperation and other bilateral security agreements.

2. APPLICABILITY. The requirements in this chapter apply to DOE personnel, covered contractors, and others who visit DOE facilities that entail access to Restricted Data and other classified information, and to DOE personnel and covered contractors that visit other specified Federal agencies.

3. REQUIREMENTS: CLASSIFIED VISIT PROCEDURES. Basic procedures for the control of all classified visits shall ensure the following:

   a. Verification of the identity and need-to-know of the visitor.

   b. The person's clearance or access authorization is at least equal to the classification of the information to which access is desired.

   c. Observance of limitations on access to classified information or facilities. Access to certain programs or information is handled in accordance with the following:

      (1) Weapons Production Programs. For access to weapons programs, nuclear materials production facilities, or sensitive nuclear materials production information, requests shall be referred to the Assistant Secretary for Defense Programs.

      (2) Uranium Enrichment. For access to uranium enrichment plants or facilities engaged in uranium enrichment technology development, including advanced isotope separation technology, the request shall be referred to the Office of Uranium Programs.

      (3) Naval Nuclear Propulsion Information. When access is desired to Naval Nuclear Propulsion Information, the request shall be referred to the Office of Naval Reactors.

   d. Timely notification of visits.

   e. Prompt transmittal of "Request for Visit or Access Approval" (DOE F 5631.20), when applicable. (This form is no longer required for DOE and DOE contractor employees who

visit DOE facilities. These employees may use their DOE picture identification badge as evidence of a DOE access authorization. However, DOE F 5631.20 is still required for programmatic approval for sigma access and for employees of other Federal agencies who visit DOE facilities.)

f. Timely notification to those concerned for approval of access to weapon data (classified Secret or Top Secret), Top Secret information (nonweapon data), sensitive nuclear materials production information, atomic vapor laser isotope separation technology, uranium enrichment technology, or facilities specifically designated by Headquarters Elements.

g. Use of continuing visitor access approval as necessary for individuals who visit DOE facilities frequently. This approval cannot exceed a period of 1 year, but the approval may be renewed annually, if necessary.

h. Operational approval of visits.

i. Maintenance of records of all classified visits by non-DOE personnel and foreign nationals.

j. Referral to the Director of Public and Consumer Affairs of any nonroutine, written, or visual material proposed for public release resulting from visits.

k. The Director of Safeguards and Security shall maintain liaison with the Department of Defense, National Aeronautics and Space Administration, and other Federal agencies in order to:

(1) ensure that DOE is notified of changes in those positions whose occupants are authorized to initiate access requests; and

(2) provide assistance in identifying DOE Elements and Federal offices to which specific requests shall be directed.

4. REQUIREMENTS: CLASSIFIED VISITS BY DOE EMPLOYEES, CONTRACTORS AND SUBCONTRACTORS.

a. The visitor is responsible for making administrative arrangements and obtaining approval from the Departmental Element, as appropriate. (The authority granting such approval is responsible for informing the office to be visited.)

b. Contractors or subcontractors with mutual program interests may be authorized, subject to the limitations in subparagraph c below, to arrange for visits without obtaining DOE approval if such authorization will be advantageous to the DOE.

c. The following procedures are required when access to weapon data (classified Secret or Top Secret), Top Secret information (nonweapon data), sensitive nuclear materials production information, inertial confinement fusion data, atomic vapor laser isotope separation

technology, uranium enrichment technology, or specific facilities designated by Headquarters Elements having program direction is required.

(1) Approval of the access during visits under the auspices of a Headquarters Element shall be obtained from the Headquarters Element exercising jurisdiction over the facility or office to be visited.

(2) Approval of this access during visits under the auspices of Field Elements shall be obtained from the responsible Field Element for field visits and for visits to Headquarters from the organization being visited.

5. REQUIREMENTS: VISITS TO DEPARTMENT OF DEFENSE AND NATIONAL AERONAUTICS AND SPACE ADMINISTRATION FACILITIES. Both agencies accept DOE access authorizations for Restricted Data and other classified information under their jurisdiction on the same basis as DOE, provided access authorization and "need-to-know" are properly certified.

a. DOE Top Secret approvals shall be specifically certified in the event access to Top Secret information is required.

b. A DOE F 5631.20, "Request for Visit or Access Approval" shall be forwarded directly to the military or civilian official with jurisdiction over the information to which access is desired.

c. Any exchange of Restricted Data occurring during the course of the visit shall be accomplished as stated in paragraph 7 below.

6. REQUIREMENTS: RESTRICTED DATA VISITS BY NUCLEAR REGULATORY COMMISSION EMPLOYEES.

a. Visits to DOE facilities by Nuclear Regulatory Commission employees, consultants, contractors, or subcontractors who require access to weapon data, sensitive nuclear materials production information, atomic vapor laser isotope separation technology, or uranium enrichment technology, or entry into a DOE classified weapon or production facility shall:

(1) be arranged through the respective Headquarters Element that will coordinate the visits;

(2) if to classified weapon or production facilities, have prior approval of the Assistant Secretary for Defense Programs;

(3) have DOE F 5631.20 or the Nuclear Regulatory Commission equivalent with necessary clearances certified by the Director of Security, Nuclear Regulatory Commission.

b. Visits involving access to other Restricted Data not requiring prior approval from the appropriate Headquarters official exercising jurisdiction over the facility or office to be visited may be arranged
directly by Nuclear Regulatory Commission with the cognizant DOE Element, provided this procedure does not conflict with the existing visitor control procedures of the division or office having program responsibility. A DOE F 5631.20 or Nuclear Regulatory Commission equivalent is required.

c. The Nuclear Regulatory Commission identification badge shall not be used as authority for visits in lieu of the aforementioned specific visit approval arrangements.

7. REQUIREMENTS: RESTRICTED DATA VISITS BY DEPARTMENT OF DEFENSE AND NATIONAL AERONAUTICS AND SPACE ADMINISTRATION EMPLOYEES.

a. Access to Restricted Data is contingent upon submission of a DOE F 5631.20, National Aeronautics and Space Administration Form-405, "Request for Access Approval," or a memorandum or electronic message signed by or in the name of the certifying official. The request shall be forwarded for approval or other action to the DOE official with jurisdiction over the information to which access is desired.

b. The request for access shall include the following:

(1) Name(s) of person(s) and organization represented (if not Armed Forces, relationship to the Department of Defense or National Aeronautics and Space Administration).

(2) Facility and information to which access is desired. Access to critical nuclear weapon design information must be specified when it is required.

(3) The security clearance or access authorization status of each person, including clearance date.

(4) Purpose of visit and certification that the person needs the access in the performance of duty.

(5) Anticipated date of visit and names of persons to be visited, as appropriate. (If a conference is involved, the date, place, and sponsor of the conference shall be specified.)

(6) Citizenship, date of birth, and social security number.

(7) For requests from National Aeronautics and Space Administration, a certification that the matter to which access is desired relates to "aeronautical and space activities."

c. The approving official must possess or have been delegated the authority to approve such access.

d. Control of access by members of the Armed Services or by Department of Defense or National Aeronautics and Space Administration personnel or contractors to Restricted Data in the custody of another Federal agency is the responsibility of the appropriate official or his/her designee named in Chapter VIII, Attachment VIII-1.

e. Headquarters Elements shall retain for 3 years a copy of each visit request they have approved. Separate records shall be maintained for approvals of access under emergency conditions.

8. REQUIREMENTS: OTHER CLASSIFIED VISITS BY DEPARTMENT OF DEFENSE AND NATIONAL AERONAUTICS AND SPACE ADMINISTRATION EMPLOYEES .

a. Requests for such visits to DOE and contractor and subcontractor facilities are approved by Heads of Field Elements or, in the case of Headquarters Elements, by the head of the element concerned after ensuring that such visitor possesses appropriate military or National Aeronautics and Space Administration security clearance and requires the information in the performance of his/her duties.

b. Certification of security clearance may be made by memorandum, electronic message, DOE F 5631.20, or National Aeronautics and Space Administration Form 405.

9. REQUIREMENTS: CLASSIFIED VISITS BY EMPLOYEES OF OTHER FEDERAL AGENCIES.

a. Requests for visits to DOE facilities by employees, contractors, or subcontractors of Federal agencies other than the Department of Defense, National Aeronautics and Space Administration, or Nuclear Regulatory Commission are approved by the Field Elements or, for Headquarters, by the organization concerned.

b. Restricted Data may not be exchanged with persons in this category unless they possess appropriate DOE access authorization.

c. Classified information other than Restricted Data may be exchanged with such individuals if they possess Q or L access authorizations or security clearances under the provisions of Executive Order 10450, "Security Requirements for Government Employment," and require the information in the performance of their duties.

10. REQUIREMENTS: CONGRESSIONAL AND STATE CLASSIFIED VISITS.

a. Requests for visits to DOE, contractor, or subcontractor facilities by members or employees of Congress or congressional committees and by Governors or their staffs may be approved by Heads of DOE Elements provided the following are established.

(1) The visitors' identities.

(2) Access authorization or security clearance.

(3) "Need-to-know."

b. The Assistant Secretary for Congressional and Intergovernmental Affairs shall be advised of requests and action taken on the requests for such visits.

11. REQUIREMENTS: EMERGENCY VISITS TO CLASSIFIED AREAS AND FACILITIES.

a. In an emergency, requests for visit approval may be made by telephone or electronic message.

b. Telephonic requests must be confirmed by memorandum or electronic message.

12. REQUIREMENTS: CLASSIFIED VISITS BY FOREIGN NATIONALS TO DOE FACILITIES. Classified visits by foreign nationals sponsored by a foreign government shall be arranged as follows.

a. If the visit is in connection with the military application of atomic energy under sections 144b and c(1) and 91c(1) or (4) of the Atomic Energy Act of 1954, as amended, the Assistant Secretary for Defense Programs shall make all arrangements for the visit, including appropriate approvals and security assurances.

b. If the visit is to the Office of Declassification in connection with the information classification program under DOE 5650.2B, the Director of Declassification shall make arrangements for the visit, including appropriate approvals and security assurances.

c. If the visit is not in connection with programs covered in the above paragraphs, the Deputy Assistant Secretary for International Energy Policy shall arrange for the visit in concert with the appropriate Headquarters staff other than those listed above, and shall coordinate with the Director of Safeguards and Security for the necessary security assurances.

d. If the visit will include discussions on naval nuclear propulsion matters, the Director of Naval Reactors shall be informed and review the visit for approval. The Director of Safeguards and Security may be requested to obtain the necessary security assurances.

e. Security assurances received under the above paragraphs shall be retained for 5 years.

13. CONTACT. Comments and inquiries on this chapter may be directed to the Personnel Security Policy Program Manager at (301) 903-3200.

ACCESS TO RESTRICTED DATA IN POSSESSION OF OTHER FEDERAL AGENCIES

The following Federal officials are authorized to permit their Federal and contractor employees possessing DOE access authorizations to grant access to Restricted Data in their possession to members of the Armed Forces and Department of Defense and National Aeronautics and Space Administration employees and their contractors, in accordance with section 143 of the Atomic Energy Act of 1954, as amended, and subsection 304(b) of the National Aeronautics and Space Act of 1958.

The Assistant to the President
Director, Office of Management and Budget
Executive Secretary, National Security Council
Director, Central Intelligence Agency
Director, Federal Emergency Management Agency

Secretary of State
Secretary of the Treasury
Attorney General of the United States
Secretary of the Interior
Secretary of Agriculture
Secretary of Commerce
Secretary of Labor
Secretary of Health and Human Services
Secretary of Transportation
Secretary of Education

Chairman, Federal Communications Commission
Administrator, Agency for International Development
President, National Academy of Sciences and National Research Council

Director, National Science Foundation
Chairman, Tennessee Valley Authority
Director, United States Information Agency

Comptroller General of the United States

CHAPTER IX

SURVEY PROGRAM

1. POLICY/OBJECTIVES. To ensure proper levels of protection consistent with Departmental standards to prevent unacceptable, adverse impact on national security or on the health and safety of DOE and contract employees, the public, or the environment are afforded safeguards and security activities. The adequacy of safeguards and security measures shall be validated through various means, such as:

   a. surveys conducted by the DOE Surveying Office prior to initiation of safeguards and security activities and periodically thereafter;

   b. periodic facility self-assessments;

   c. program reviews by Facility Survey Operations Managers and other appropriate Departmental Elements; and

   d. inspections and assessments by the Deputy Assistant Secretary for Independent Oversight and Appraisals.

2. APPLICABILITY. The Survey Program applies to all facilities that are eligible to have access to, use, store, or transmit nuclear and other hazardous material presenting a potential radiological or toxicological sabotage threat and/or classified information, that require access authorizations, or that possess over $5,000,000 of DOE property, exclusive of facilities and land values.

3. TYPES OF SURVEYS.

   a. Initial. A comprehensive survey conducted at the facility before granting approval.

   b. Periodic. A comprehensive survey conducted at the facility at scheduled intervals.

   c. Special. A survey conducted at the facility for a specific, limited purpose such as for a technical security reason (i.e., Technical Surveillance Countermeasures surveys or services), a detailed review of a problem area, an unannounced survey, shipment of nuclear materials or classified material, or change in the contractor operating a government-owned facility. Shipments between sites by rail, truck, air, or ship are subject to survey unless the shipment is made via commercial carrier licensed by the Nuclear Regulatory Commission.

   d. Termination. A survey of a facility conducted when all safeguards and security activities have been removed, access authorizations terminated, and close out of required records accomplished, to ensure proper disposition of classified matter and nuclear and other hazardous material presenting a potential radiological or toxicological sabotage threat. Termination of facility clearances for facilities possessing Top Secret matter or special nuclear

material require an onsite termination survey. For other facilities, termination may be by onsite survey or correspondence.

4. SCOPE OF SURVEYS.

a. Compliance. The compliance segment of a facility survey reflects the status of a facility's safeguards and security system as measured against implementation of applicable Federal statutes, regulations, policy, and approved safeguards and security plans.

b. Performance. The performance segment of a facility survey reflects the degree to which the elements of the safeguards and security system meet protection objectives based upon operational testing of the system.

c. Comprehensive. Comprehensive surveys cover the protection afforded safeguards and security activities and interests within a facility, including an evaluation of the adequacy and effectiveness of safeguards and security programs and a thorough examination of policies and procedures to ensure compliance and performance. All applicable topical areas, identified on DOE F 5634.1, "Safeguards and Security Survey Report," must be surveyed, except as identified in paragraph 5c.

d. Other. The scope of special and termination surveys shall be determined by coordination between the Lead Responsible Office and the Surveying Office. The basis for scope determinations shall be established by the nature or status of operations at the facility, activity, or element being surveyed. These surveys need not cover all topical areas identified on DOE F 5634.1.

5. REQUIREMENTS: FREQUENCY OF SURVEYS.

a. Initial surveys are not required for non-possessing facilities. Termination surveys of non-processing facilities are not required; however, a review shall be conducted and documented to verify that access authorizations have been terminated.

b. Periodic surveys shall be conducted in accordance with the following schedule.

(1) Facilities possessing classified matter or Category III or greater nuclear and other hazardous material presenting a potential radiological or toxicological sabotage threat shall be surveyed once every 12 months.

(2) Facilities possessing property protection interests shall be surveyed once every 24 months.

(3) Facilities that do not possess classified matter but do issue access authorizations to employees to satisfy contractual obligations shall be reviewed at least once every 5 years and not necessarily through an on-site survey. The review shall validate access authorizations and FOCI information.

(4) For facilities containing only Category IV nuclear materials as defined in DOE 5633.3B, the materials control and accountability topical area shall be surveyed at least once every 24 months. If the total inventory consists entirely of source material, less than 10 tons of heavy water, less than 350 grams of special nuclear materials, or any combination of these, a survey of the materials control and accountability topical area is not required.

c. The results of prior surveys may affect the scheduling frequency. An extended survey schedule (up to 24 months) may be implemented by the Surveying Office after consultation with the Lead Responsible Office if the facility has:

(1) a facility security staff trained and knowledgeable in safeguards and security requirements, as evidenced by past performance in surveys;

(2) an ongoing self-assessment program covering all survey topics and sub-topics with the results reported to the Lead Responsible Office;

(3) no significant deficiencies resulting from self-assessments or surveys (including no less than a satisfactory rating at the topic levels); and

(4) an approved site safeguards and security plan.

Schedules for facilities with Category I special nuclear materials may be extended if all conditions above have been met.

d. Reviews, including inspections, conducted by Departmental Elements other than the Surveying Office or other Government oversight offices, may be used to meet survey requirements. Topics and subtopics on DOE F 5634.1 that are not addressed during reviews must be surveyed by the Surveying Office. When using reviews to meet the requirements of the survey, the following guidelines shall be followed.

(1) The review must have been conducted within the surveyed period.

(2) Portions of the review used must be attached to the survey.

(3) Topics and subtopics not covered by the review must be surveyed.

(4) If ratings were not assigned, ratings must be assigned for those reviews that are used. After the review is conducted, the Surveying Office shall analyze the impact of any deficiencies and assign ratings.

e. Special surveys shall be conducted as determined by the Lead Responsible Office.

6. REQUIREMENTS: SURVEY CONDUCT.

   a. Survey Responsibility. The Lead Responsible Office must ensure surveys are conducted. The responsibility for conducting surveys may be transferred to another Surveying Office and documented on DOE F 5634.3. Secretarial Officers shall function as the Surveying Office for those offices identified in Chapter I, paragraph 7, by ensuring that periodic surveys are completed. Lead Responsible Offices for facilities that ship nuclear materials are responsible for conducting shipment surveys.

   b. Survey Team Composition. Survey teams are composed of inspectors and support service personnel. All survey teams shall be led by a Federal employee. Team personnel for surveys shall possess qualifications, experience, and training sufficient to accomplish effective and thorough surveys. New inspectors must attend basic survey training.

   c. Planning. The survey process and requirements shall be documented in locally approved survey guidelines. Surveying Offices shall coordinate planning with the Lead Responsible Office and other organizations with registered safeguards and security activities.

   d. Coordination of Surveys.

      (1) Safeguards and security surveys should be conducted in an integrated manner. If performed separately, the Surveying Office shall document the responsibility for each survey activity and coordinate submission of a single survey report that includes a composite facility rating.

      (2) Survey field activities conducted separately must be completed within 30 working days of each other, except as identified in paragraph 3c above.

   e. Validation. To ensure accuracy, survey results shall be validated by discussion, observations, or exercises during the survey period.

   f. Closeout. A final closeout briefing shall be conducted with the surveyed organization to present, at a minimum, the following items.

      (1) Each finding.

      (2) Topical ratings and the overall composite rating.

      (3) Corrective action reporting requirements.

7. REQUIREMENTS: SURVEY REPORTS.

a. Report Content. Reports shall describe the conduct, results, and evaluation of the safeguards and security program and shall include the following minimum requirements.

(1) A completed DOE F 5634.1.

(2) An executive summary containing:

(a) a statement reflecting survey scope, period of coverage, and survey methodologies used;

(b) a description of the facility, function, and scope of operations;

(c) a discussion of major points that had, or might have, a significant effect on the facility's safeguards and security program, including strengths, weaknesses, and the correlation of results from the survey; and

(d) the overall composite facility rating with supporting rationale.

(3) The report, which must include:

(a) a copy of the current DOE F 5634.3;

(b) identification of each active DOE F 5634.2 (or DD 254);

(c) a description of the facility's safeguards and security program by topical area as identified on the DOE F 5634.1;

(d) the methodology used to evaluate the facility;

(e) a description of the function and scope of operations and the protective measures employed (descriptions in safeguards and security plans may be referenced when no changes have occurred);

(f) identification of all new findings;

(g) the status of corrective actions for all open findings and status of all open and closed findings from the previous survey;

(h) concluding analysis of each topical area; and

(i) a justification and rationale of the factors responsible for the composite facility rating.

b. Termination Survey Reports. Termination survey reports shall include the following minimum information/reported action.

(1) Verification of non-possession of classified matter or nuclear and other hazardous material presenting a potential radiological or toxicological sabotage threat.

(2) Verification that personnel access authorizations no longer needed have been canceled and validation that termination statements have been completed by affected employees.

(3) Verification of deletion of all safeguards and security activities.

(4) Termination of facility clearance.

c. Distribution. Within 60 working days after final closeout of the survey, the Surveying Office shall distribute the final survey report to all Departmental Elements with a registered activity and to all appropriate Headquarters Elements. For Departmental Elements or other government agencies with limited safeguards and security activities, survey results may be transmitted by memorandum.

8. REQUIREMENTS: RATING SYSTEM. The composite facility rating shall be based on the effectiveness and adequacy of the safeguards and security at a facility and reflect a balance of performance and compliance as determined by the Surveying Office. Ratings are not assigned for termination surveys.

a. Types of Ratings.

(1) Satisfactory. The safeguards and security element being evaluated meets protection objectives or provides plausible assurance that protection needs are being met.

(2) Marginal. The safeguards and security element being evaluated only partially meets protection objectives or provides questionable assurance that protection needs are being met.

(3) Unsatisfactory. The safeguards and security element being evaluated does not meet protection objectives or does not provide adequate assurance that protection needs are being met.

b. Basis for Ratings.

(1) Ratings are based on conditions existing at the end of survey activities. Ratings shall not be based upon future or planned corrective actions.

(2) If corrective actions are taken before assignment of the survey rating at closeout, the final rating shall reflect validated corrective actions only.

(3) Marginal or unsatisfactory ratings in any topical area shall be based on validated weaknesses in the safeguards and security system or deficiencies in performance in an

operational area. Failure to comply with procedural documentation requirements, of and by itself, shall not normally be the basis for a reduction in a rating.

c. Use of Marginal Ratings. A facility composite rating or topical area rating shall not be marginal for consecutive survey periods unless one of the following conditions apply.

(1) The previous survey that resulted in a marginal rating identified different deficiencies and reasons for the rating.

(2) The deficiencies and reasons that were the basis for the previous marginal rating were related to the completion of a major line-item construction project or upgrade program. In that case, acceptable interim measures must have been implemented and physically validated pending completion of the project. These interim measures and milestones for construction completion shall be documented in the survey report.

(3) If neither of the above conditions apply, an unsatisfactory rating shall be assigned.

d. Survey Report. Ratings shall be based on the impact of deficiencies. All ratings must be stated and justified in the survey report.

9. REPORTING REQUIREMENTS: MARGINAL AND UNSATISFACTORY COMPOSITE RATINGS. Reporting requirements identified below are initiated by the final close-out briefing.

a. Marginal. Within 15 working days following a survey closeout that results in an overall composite rating of marginal, the Lead Responsible Office shall notify the Office of Safeguards and Security, and the applicable Departmental Elements. Notification shall contain the following.

(1) Identification of the facility (including both the facility code and reporting identification symbol - if applicable).

(2) A list of findings describing the deficiencies.

(3) A description of corrective actions taken to date or planned with associated milestones.

(4) A justification statement addressing the overall composite rating and status of the safeguards and security program at the facility.

(5) A statement identifying risks or vulnerabilities.

(6) A statement acknowledging physical validation of adequacy of interim corrective actions taken to date.

(7) A statement outlining steps that shall lead to the upgrading of the overall composite rating to satisfactory.

If the Surveying Office is not the same as the Lead Responsible Office, the Surveying Office shall notify the Lead Responsible Office of results and rating(s) within 72 hours of survey closeout. The Lead Responsible Office shall then take corrective and notification actions outlined in this chapter or authorize the Surveying Office to take those actions.

If the Surveying Office is unable to contact the Lead Responsible Office and a serious threat exists or is imminent, the Surveying Office shall take action to protect safeguards and security activities until the Lead Responsible Office can be notified. Subsequent action shall be taken on the basis of agreement between the two organizations and shall be fully documented in the survey report.

b. Unsatisfactory. When a survey results in an overall composite rating of unsatisfactory, the Operations Office Manager of the Lead Responsible Office shall coordinate with Secretarial Officers and other Heads of Operations Offices within 24 hours to:

(1) take action to suspend the activity and/or the facility clearance pending remedial action or

(2) provide the rationale for continuing this critical operation to the Office of Security Affairs, the Office of Safeguards and Security, Secretarial Officers, and as directed, applicable Operations Offices. In addition to providing the rationale, the Lead Responsible Office must identify those immediate interim corrective actions being undertaken to mitigate identified risks or vulnerabilities.

If the Surveying Office is not the same as the Lead Responsible Office, the Surveying Office shall notify the Lead Responsible Office of the results and rating(s) within 8 hours of survey closeout.

If the Surveying Office is unable to contact the Lead Responsible Office, action shall be taken to protect safeguards and security activities until the Lead Responsible Office can be notified. Subsequent action will be taken on the basis of agreement between the two organizations and shall be fully documented in the survey report.

c. Change of Rating. When the Lead Responsible Office determines that the composite survey rating shall be upgraded, the Lead Responsible Office shall then notify the Office of Safeguards and Security and the appropriate Secretarial Officer.

10. REQUIREMENTS: CORRECTIVE ACTIONS.

a. When a survey contains findings, the surveyed organization shall submit a response identifying corrective action(s) for each finding to the Responsible and Surveying Offices no later than 30 working days after formal receipt of findings. The corrective action(s) should be based on documented root cause analysis, risk assessment, and cost-benefit analysis.

b. When a survey indicates a composite rating of satisfactory but contains findings requiring corrective action, the Lead Responsible Office shall enter the findings and status of corrective actions in the Safeguards and Security Information Management System and quarterly provide electronic status notification to the Office of Safeguards and Security, the appropriate Secretarial Officers, and the Surveying Office (if appropriate).

c. When a survey has a composite rating of marginal, the Lead Responsible Office shall notify the Director, Office of Safeguards and Security, the Surveying Office (if appropriate), and the applicable Operations Office and Secretarial Officer(s) within 15 working days after completion of the survey.

(1) The notification must address interim corrective actions taken, or to be taken, to correct identified risks or vulnerabilities.

(2) If interim corrective actions are instituted, the Surveying Office shall physically verify them for adequacy.

(3) If the Surveying Office is not the same as the Lead Responsible Office, the Surveying Office shall promptly notify the Lead Responsible Office of the rating. The Lead Responsible Office shall then take appropriate corrective and notification actions outlined above or authorize the Surveying Office to take those actions.

(4) If the Surveying Office is unable to contact the Lead Responsible Office and a serious threat exists or is imminent, the Surveying Office shall take action to protect the safeguards and security interest(s) until the Lead Responsible Office is notified. Subsequent action shall be taken on the basis of agreement between the two organizations.

d. When a survey has a composite rating of unsatisfactory, and the rating indicates a significant vulnerability, such as unacceptable risk of special nuclear material theft, radiological sabotage, toxicological sabotage, or industrial sabotage or espionage, the Operations Office Manager shall coordinate with the cognizant Program Secretarial Officer 24 hours to:

(1) take action to shut down/suspend operation of the facility or activity, pending remedial action or

(2) apprise the cognizant Secretarial Officer and the Office of Safeguards and Security of the rationale for continuing this critical operation and identify those immediate interim corrective actions being undertaken to mitigate identified risks or vulnerabilities.

For all other unsatisfactory ratings, the Operations Office Manager of the Lead Responsible Office shall notify the cognizant Secretarial Officer and the Office of Safeguards and Security within 15 working days of interim corrective actions taken, or to be taken, to correct identified risks or vulnerabilities.

e. When either a marginal or unsatisfactory composite rating is assigned, the Lead Responsible Office shall provide to the Office of Safeguards and Security and the applicable Operations Office and Secretarial Officer(s) quarterly status reports on completed or planned corrective actions (with associated milestone dates) until all have been completed. When the Lead Responsible Office determines that the composite survey rating should be upgraded to satisfactory, the Surveying Office shall physically verify the completion and adequacy of corrective actions. The Lead Responsible Office shall then notify the Director, Office of Safeguards and Security, and the Cognizant Secretarial Officer(s) that the rating should be upgraded.

f. A finding associated with a significant vulnerability shall not be considered closed until associated corrective action has been completed and the Office of Safeguards and Security and the Secretarial Officer(s) are notified. A commitment by the facility to institute corrective action does not constitute completion of that corrective action.

11. CONTACT. Comments and inquiries regarding this chapter may be directed to the Technical and Operations Security Program Manager at (301) 903-5217.

CHAPTER X

SELF-ASSESSMENT PROGRAM

1. OBJECTIVE. A safeguards and security self-assessment program shall be implemented to ensure internal monitoring of compliance and performance with safeguards and security requirements.

2. APPLICABILITY. This program applies to Departmental and contractor facilities for which a DOE F 5634.3 is recorded. The level of detail of the self-assessment may be specified by the Lead Responsible Office.

3. REQUIREMENTS.

   a. Self-assessment programs shall be conducted and documented for all approved facilities. The self-assessment program shall:

      (1) include reviews of all applicable DOE F 5634.1 topical and subtopical areas of the facility's safeguards and security program/system;

      (2) be conducted between the periodic surveys conducted by the Surveying Office; and

      (3) be conducted using personnel knowledgeable of the programmatic or topical area.

   b. Self-assessment reports shall:

      (1) address reviewed topical areas;

      (2) be used as organizational management tools/aids in determining the status of safeguards and security performance and compliance with applicable safeguards and security Order requirements;

      (3) be available for review by the Surveying Office during surveys; and

      (4) list findings resulting from self-assessment activities.

   c. Findings resulting from self-assessments shall be processed as follows.

      (1) Reviewed during the surveys by the Surveying Office.

      (2) Addressed by facility/organization management through a documented corrective action plan.

      (3) Reviewed and the status of findings tracked until closed.

(4) Reported to the Lead Responsible Office if:

(a) a vulnerability to national security, classified information, nuclear materials, or Departmental property results, or may result, in a significant anomaly that could have significant programmatic impact or embarrass the Department; or

(b) the self-assessment is used to extend the Surveying Office's periodic survey frequency.

(5) Documented in survey reports when deficiencies still exist and have not been adequately addressed.

4. CONTACT. Comments and inquiries regarding this chapter may be directed to the Technical and Operations Security Program Manager at (301) 903-5217.

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

PAGE CHANGE

DOE O 470.1 Chg 1

6-21-96

SUBJECT: SAFEGUARDS AND SECURITY PROGRAM

1. PURPOSE. To transmit revised pages to DOE O 470.1, SAFEGUARDS AND SECURITY PROGRAM, of 9-28-95.

2. EXPLANATION OF CHANGES. To clarify that persons seeking unescorted access to security areas must receive an initial briefing, and sign the Classified Information Nondisclosure Agreement before access to classified information is granted. In addition, a Manual to supplement this Order will be published in lieu of a Guide.

3. FILING INSTRUCTIONS.

a.	Remove Pages	Dated	Insert Pages	Dated
	IV-l to IV-4	9-28-95	IV-1 to IV-4	6-21-96

b. After filing the attached pages, this transmittal may be discarded.

BY ORDER OF THE SECRETARY OF ENERGY:

ARCHER L. DURHAM
Assistant Secretary for
Human Resources and Administration

DISTRIBUTION:
All Departmental Elements

INITIATED BY:
Office of Human Resources
and Administration