7-23-93

E X P L A N A T I O N S H E E T

DOE 5639.8A, SECURITY OF FOREIGN INTELLIGENCE INFORMATION AND SENSITIVE COMPARTMENTED INFORMATION FACILITIES, HAS REVISED DOE 5639.8 TO CLARIFY RESPONSIBILITIES AND AUTHORITIES ASSIGNED TO THE OFFICES OF INTELLIGENCE AND SECURITY AFFAIRS AND REFLECT CHANGES IN ORGANIZATIONAL TITLES AS A RESULT Of THE RECENTLY APPROVED DEPARTMENTAL REALIGNMENT. NO OTHER SUBSTANTIVE CHANGES HAVE BEEN MADE.

THIS EXPLANATION SHEET MAY BE RETAINED FOR REFERENCE OR DISCARDED.

U.S. Department of Energy

Washington, D.C.

ORDER

DOE 5639.8A

7-23-93

SUBJECT: SECURITY OF FOREIGN INTELLIGENCE INFORMATION AND SENSITIVE COMPARTMENTED INFORMATION FACILITIES

1. POLICY. To establish responsibilities and authorities for protecting Foreign Intelligence Information (FII) and Sensitive Compartmented Information Facilities (SCIFs) within the Department of Energy (DOE).

2. CANCELLATION. DOE 5639.8, SECURITY OF FOREIGN INTELLIGENCE INFORMATION AND SENSITIVE COMPARTMENTED INFORMATION FACILITIES, of 9-15-92.

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

4. APPLICABILITY. This Order applies to all DOE Elements, including DOE-owned, contractor-operated and/or subcontractor-operated activities performing work for the Department which require access, receipt, storage, processing and/or handling of Foreign Intelligence Information. DOE Elements shall follow the provisions, policies, procedures, responsibilities and authorities detailed in this Order. which are applicable to properly establish, manage, and operate facilities which receive, store, process, aid disseminate FII, including Sensitive Compartmented Information (SCI).

5. REFERENCES. See Attachment 1.

6. DEFINITIONS. See Attachment 2.

7. POLICY. The security afforded DOE foreign intelligence information and activities shall not pose an unacceptable risk to the national security, and security shall conform to the applicable provisions of Executive Order 12333, 'United States Intelligence Activities," of 12-4-81; Executive orders as may supersede it; and to applicable Director of Central Intelligence Directives (DCID).

8. RESPONSIBILITIES AND AUTHORITIES.

   a. The Secretary is the Senior Official of the Intelligence Community (SOIC).

   b. Heads of Departmental Elements shall:

      (1) Require contractors, through the contracting officer(s), to conduct FII activities in accordance with this Order and other appropriate policy

DISTRIBUTION:
All Departmental Elements

INITIATED BY:
Office of Safeguards and Security

and procedural documents published by the DOE for management and operation of facilities and activities associated with control and accountability of FII, to include SCI.

(2) Designate an individual (s) to be responsible for bringing to the attention of the contracting officer 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 Authorization Request").

c. D)irector of Intelligence and National Security through:

(1) Director of Security Affairs shall, in coordination with the Director of Intelligence:

(a) Develop overall Departmental security policy and procedures for the protection of FII and SCI in accordance with DCIDs 1/7, 1/14, 1/16, 1/19, 1/20, 1/21, 1/22, and associated appendices.

(b) In the area of personnel security:

1 Develop security policy and procedures applicable to SCI access eligibility.

2 Adjudicate background investigations and reinvestigations and provide security determinations to the Director of Intelligence on individual's eligibility for access to SCI.

3 Manage the continuing security education briefing and awareness program through development of educational materials and ensure refresher briefings are conducted in compliance with established Orders.

(c) In the area of information security:

1 Develop security policy and procedures for the protection of classified information containing foreign intelligence information.

2 Conduct security inquiries involving actual or suspected incidents involving a possible or probable compromise of FII, including SCI.

3 Conduct periodic inspections at Headquarters to ensure compliance with security procedures for the receipt, control, dissemination, transmission, and destruction of FII. These inspections will not include access to specific compartmented information or program activities unless specified by the SOIC.

(d) In the area of physical/technical/automated information systems (AIS).

1 Develop security policy, procedures, standards, and criteria for new construction or modification of existing SCIFs, and

advise the Director of Intelligence on the status of new construction or modifications to existing SCIFs.

2 Conduct preconstruction review and formally inspect/evaluate new construction or modifications to existing SCIFs, and provide the final accreditation package and certification to the Director of Intelligence for final accreditation.

3 Develop security policy and procedures for the physical, technical, AIS and networks which support SCIFs as they apply to DOE and its contractor-operated facilities relative to FII.

4 Review and approve written certification of compliance with approved AIS and general security plans, equipment, and installation criteria and associated SCIF standard operating procedures and emergency plans, and provide these plans and certifications as part of the final SCIF accreditation package to the Director of Intelligence for final accreditation or reaccreditation as appropriate.

(e) In addition to the above responsibilities, carry out the responsibilities outlined in paragraph 8b, above.

(2) Director of Intelligence, as the Senior Intelligence Officer (SIO) and the Secretary's executive agent for implementation and monitoring the provisions of Executive Order 12333, shall:

(a) Develop intelligence policy and procedures for FII and SCI.

(b) Approve access to FII, including SCI, for DOE and DOE contractor personnel.

(c) Control the use and dissemination of foreign intelligence, including SCI, by DOE Elements and their contractors in accordance with directives from and/or agreements with the Intelligence Community (IC).

(d) Approve requests for construction of *new* SCIFs or modifications to existing SCIFs in accordance with directives from and/or agreements with the IC.

(e) Accredit all DOE SCIFs and their inherent systems which have been certified by the Director of Safeguards and Security, in accordance with directives from and/or agreements with the IC.

(f) Maintain a master security file on each SCIF.

(g) In the area of personnel security:

1 Receive all requests from DOE Elements and their contractors for SCI access; approve or disapprove the need-to-know; and formally request eligibility data from the Director of Safeguards and Security.

2 Receive security determinations from the Director of Safeguards and Security relative to background investigations; determine individual eligibility for access to SCI; and direct indoctrination proceedings for DOE and its contractor personnel.

3 Maintain formal records of SCI indoctrinations and special accesses for DOE and its contractor/subcontractor personnel and acts as the formal channel for receiving and passing SCI security clearance information.

4 Assist the Director of Security Affairs, as required, in developing educational materials designed to provide an adequate and effective security awareness and education program for those persons who have been authorized access to FII.

5 Coordinate with the Director of Security Affairs to establish channels for the exchange of information bearing on the security posture of persons having access to FII.

(h) In the area of information security:

1 Develop, in coordination with the Director of Security Affairs, procedures and systems for protection of FII held within DOE and contractor/subcontractor facilities.

2 Provide substantive inputs to the Director of Security Affairs on new or revised IC security policies and procedures relative to FII.

3 Conduct periodic inspections of document markings, accountability, and inventory of SCI holdings in accordance with established policy and procedural guidance.

(i) In the area of physical/technical/AIS security:

1 Coordinate with the Director of Security Affairs on requests for new construction or modifications to existing SCIFs, and assist the Director of Security Affairs in the evaluation process relative to certification of DOE SCIFs.

2 Support the Deputy Assistant Secretary for Security Evaluations in the conduct of SCIF inspections and evaluations by assisting with that portion of the evaluation dealing with the receipt, control, dissemination, storage, and destruction of SCI.

(j) In coordination with the Director of Security Affairs and the Deputy Assistant Secretary for Security Evaluations, prepare a master schedule of inspections/evaluations for DOE accredited SCIFs and ensure the conduct of inspections/evaluations of the security posture of each SCIF a minimum of once every year.

(k) Provide copies of SCIF inspection/evaluation reports to affected Secretarial Officers, the Director of Security Affairs, Heads of Field Elements, and affected SCIFs.

(1) In addition to the above responsibilities, carry out the responsibilities outlined in paragraph 8b, above.

d. Deputy Assistant Secretary for Security Evaluations shall:

(1) Direct, manage, and conduct independent inspections, performance tests, and evaluations to assess the protection program and the effectiveness of the levels of protection and compliance with regulations, requirements, and Orders at DOE facilities.

(2) Evaluate the effectiveness of DOE policies and programs for meeting requirements of applicable statutes and Executive orders.

(3) Advise Heads of Departmental Elements on the security posture of DOE Elements and their contractor-operated facilities with respect to compliance with DOE policies and directives.

(4) In addition to the above responsibilities, carry out the responsibilities outlined in paragraph 8b, above.

e. Assistant Secretary for Human Resources and Administration shall:

(1) Assist the Director of Intelligence in the development and execution of viable communications security (COMSEC) and TEMPEST activities related to FII and SCI.

(2) Provide technical advice and assistance relative to the installation of equipment used to process or store foreign intelligence information, to include SCI, and assist the Director of Security Affairs to properly analyze and evaluate the security risks associated with approving the facility for continued operation.

(3) Assist the Director of Security Affairs during inspections, evaluations, surveys, and assessments to verify adequate installation of equipment and other technical areas.

(4) Assist the Director of Security Affairs during the Internal Review Budget process by assuring that adequate integrated security systems are planned, designed, and constructed for all DOE facilities.

(5) In addition to the above responsibilities, carry out the responsibilities outlined in paragraph 8b, above.

f. Heads of Field Elements shall:

(1) Ensure requests for SCI access from their organizations, including contractors, provide the information required, including the need-to-know justification, prior to being forwarded to the Director of Intelligence.

(2) Ensure the inspection of DOE security facilities to assure the security of DOE and DOE-owned, contractor-operated, and subcontractor-operated facilities, including SCIFs, under their jurisdiction in accordance with established policy and procedural guidance.

(3) Develop, in coordination with the Director of Security Affairs, policy and procedures to ensure that an adequate and viable security program exists for the protection of FII, to include SCI, located in DOE and DOE-owned contractor-operated and subcontractor-operated facilities under their jurisdiction.

(4) Provide to the Director of Security Affairs site approved, preconstruction architectural and engineering design materials, and results of the local DOE security element review. Any recommendations developed through the local review of proposed construction of new SCIFs or modifications to existing SCIF(s) shall be submitted to the Director of Security Affairs for approval prior to beginning any construction or modification activities.

(5) Review cognizant SCIF AIS and general security plans and standard operating procedures and any changes/revisions to existing plans for adequacy and compliance with established policies and directives, and forward plans to the Director of Security Affairs and the Director of Intelligence for appropriate action.

(6) Provide local support to the Deputy Assistant Secretary for Security Evaluations, the Director of Security Affairs, and the the Director of Intelligence during the conduct of evaluations of cognizant SCIF(s), as required.

(7) Request the Director of Security Affairs support in correcting any physical, technical, or operational security deficiencies on DOE-owned facilities under their jurisdiction.

(8) Ensure the immediate notification of the Director of Security Affairs and the Director of Intelligence on possible or probable compromises of both collateral FII and SCI.

(9) In addition to the above responsibilities, carry out the responsibilities outlined in paragraph 8b, above.

g. Director, Naval Nuclear Propulsion Program shall, in accordance with the responsibilities and authorities assigned by Executive Order 12344 (statutorily prescribed by Public Law 98-525 (42 United States Code (U.S.C.), 7158, note) and to ensure consistency throughout the joint Navy/DOE organization of the Naval Nuclear Propulsion Program, implement and oversee all policy and practices pertaining to this Order for activities under the Director’s cognizance.

h. Procurement Request Originators (the individuals responsible for initiating a requirement on DOE F 4200.33), or such other individual(s) as designated by the cognizant Head of the Departmental Element, shall bring to the attention of the cognizant contracting officer the following: (1) each procurement requiring the application of this Order; (2) requirement for flow down of provisions of this Order to a subcontractor; and (3) identification of the paragraphs of this Order with which the contractor or, if different, subcontractor is to comply.

i. Contracting Officers, based on advice received from the procurement request originator or other designated individual, shall apply applicable provisions of this Order to contracts falling within its scope. For contracts other than management and operating contracts, this shall be by incorporation or reference using explicit language in a contractual action, usually bilateral.

BY ORDER OF THE SECRETARY OF ENERGY:

ARCHER L. DURHAM
Assistant Secretary for Human
Resources and Administration

REFERENCES

NOTE: Director of Central Intelligence Directives (DCIDs) are provided to DOE field elements for reference only. The applicable portions of these documents are or will be incorporated in Orders or procedural guides as appropriate.

1. Executive Order 12333, "United States Intelligence Activities," of 12-4-81, which sets forth the goals, direction, duties, and responsibilities with respect to the National Intelligence effort.

2. Executive Order 12356, "National Security Information," of 4-2-82, which provides requirements for safeguarding National Security Information, and Information Security Oversight office Directive No. 1, of 6-25-82, which assists in implementing Executive Order 12356.

3. Title 42, United States Code (U.S.C.), 2011 et seq., Atomic Energy Act of 1954, as amended, which describes requirements for the protection of classified information relating to atomic energy.

4. DOE 5670.1A, MANAGEMENT AND CONTROL OF FOREIGN INTELLIGENCE, of 1-15-92, which establishes guidelines for management of, and assigns responsibilities for, the foreign intelligence activities of DOE.

5. DOE 5631.1B, SECURITY EDUCATION BRIEFING AND AWARENESS PROGRAM, of 12-31-91, which establishes policies, responsibilities, and requirements for the implementation of a security education program for the Department of Energy.

6. DOE 5631.2C, PERSONNEL SECURITY PROGRAM, of 9-15-92, which establishes the policies, responsibilities, and authorities for implementing the personnel security program.

7. DOE 5632,1B, PROTECTION PROGRAM OPERATIONS, of 9-8-92, which establishes policy, responsibilities, and authorities for the physical protection of security interests.

8. DOE 5639.5, TECHNICAL SURVEILLANCE COUNTERMEASURES PROGRAM, of 8-3-92, which establishes the technical surveillance countermeasures program.

9. DOE 5639.6, CLASSIFIED COMPUTER SECURITY PROGRAM, of 9-15-92, which establishes responsibilities and procedures for developing and implementing a program to ensure the security of information stored in classified ADP systems.

10. DOE 5300.2D, TELECOMMUNICATIONS: EMISSION SECURITY (TEMPEST) , of 5-18-92, which establishes the telecommunications program for emission security.

11. DOE 5300.3C, TELECOMMUNICATIONS: COMMUNICATIONS SECURITY, of 5-18-92, which establishes policy, responsibilities, and guidance related to communications security.

12. DOE 5300.4C, TELECOMMUNICATIONS: PROTECTED DISTRIBUTION SYSTEMS, of 5-18-92, which provides guidance on systems used to transmit classified or sensitive unclassified information.

13. DOE Procedural Guide, "Security of Foreign Intelligence Information and Sensitive Compartmented Information Facilities" (Formerly Security Standards for Sensitive Compartmented Information and Facilities), of 1-1-85, which implements the appropriate portions of DCIDs. This guide is available from the Headquarters Office of Safeguards and Security.

14. Director of Central Intelligence Directive (DCID) 1/7, "Security Controls on the Dissemination of Intelligence Information," of 1-7-84, which establishes policies, controls, and procedures for the dissemination and use of intelligence information and materials bearing the Director of Central Intelligence (DCI) authorized control markings.

15. DCID 1/14, "Minimum Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information," of 11-27-84, which enhances the security protection of SCI through standards, procedures, security programs, and a facilitated security certification process among Department/agencies.

16. DCID 1/16, "Security Policy on Intelligence Information in Automated Systems and Networks," of 1-4-83, which establishes policies and procedures for the security of classified intelligence information processed or stored in automated systems and networks.

17. DCID 1/19, "Security Policy for Sensitive Compartmented Information," of 6-28-82, which establishes policies and procedures for the security, use, and dissemination of SCI.

18. DCID 1/20, "Security Policy Concerning Travel and Assignment of Personnel with Access to Sensitive Compartmented Information," of 3-11-85, which establishes the minimum policy concerning assignment and travel of U.S. Government civilian and military personnel, government consultants and employees of government contractors who have, or who have had, access to SCI.

19. DCID 1/21, "Physical Standards for Sensitive Compartmented Information Facilities," of 9-1-87, which establishes minimum construction and security protection for all U.S. Government facilities or U.S. Government-sponsored contractor facilities where SCI may be stored, used, discussed, and/or processed.

20. DCID 1/22, "Technical Surveillance Countermeasures," of 7-3-85, which establishes the policy and procedures for the conduct and coordination of technical surveillance countermeasures.

DEFINITIONS

1. CLASSIFIED INFORMATION. Certain information requiring protection against unauthorized disclosure in the interests of national defense and security or foreign relations of the United States pursuant to Federal statute or Executive order. The term includes Restricted Data, Formerly Restricted Data, and National Security Information. The potential damage to the national security of each is denoted by the classification levels Top Secret, Secret, or Confidential.

2. CONTRACTORS AND SUBCONTRACTORS. For the purpose of this Order, contractors and subcontractors are those contractors performing work for the Department of Energy (DOE) which is associated with DOE foreign intelligence activities.

3. FOREIGN INTELLIGENCE INFORMATION (FII) . For the purpose of this Order, Foreign Intelligence Information is National Security Information relating to the capabilities, intentions and activities of foreign powers, organizations or persons, which carry the following special caveats for control and access:

   a. WNINTEL = Warning Notice - Intelligence Sources and Methods Involved.

   b. NOCONTRACT = Not Releasable to Contractors/Consultants.

   c. ORCON = Dissemination and Extraction of Information Controlled by Originator.

4. FORMERLY RESTRICTED DATA (FRD). Classified information jointly determined by DOE or its predecessors and DOD to be related primarily to the military utilization of atomic weapons, and removed by DOE from the Restricted Data category pursuant to Section 142(d) of the Atomic Energy Act of 1954, as amended, and safeguarded as National Security Information, subject to the restrictions on transmission to other countries and regional defense organizations that apply to Restricted Data.

5. INTELLIGENCE COMMUNITY. Those United States Government organizations and activities identified in Executive Order 12333 or successor orders as comprising the intelligence community.

6. NATIONAL SECURITY INFORMATION (NSI). Any information that has been determined pursuant to Executive Order 12356 or any predecessor order to require protection against unauthorized disclosure and that is so designated. The levels TOP SECRET, SECRET, AND CONFIDENTIAL are used to designate such information.

7. RESTRICTED DATA (RD). All data concerning: design, manufacture, or utilization of atomic weapons; the production of special nuclear material; or the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to Section 142 of the Atomic Energy Act of 1954, as amended.

8. SENSITIVE COMPARTMENTED INFORMATION (SCI). Classified Information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence.

9. SENSITIVE COMPARTMENTED INFORMATION FACILITY (SCIF). An accredited area, room, group of rooms, or installation where Sensitive Compartmented Information may be stored, used, discussed, and/or electronically processed.

10. SPECIAL ACCESS PROGRAM (SAP). Any program established under Executive Order 12356 or the Atomic Energy Act of 1954, as amended, that imposes additional controls governing access to classified information involved with such programs beyond those required by normal management and safeguarding practices. These additional controls may include, but are not limited to, access approval, adjudication or investigative requirements, special designation of officials authorized to determine a need-to-know, or special lists of persons determined to have a need-to-know.