U.S. Department of Energy

Washington, D.C.

ORDER

DOE 5670.3

9-4-92

SUBJECT: COUNTERINTELLIGENCE PROGRAM

1. PURPOSE. To establish the policies, procedures, and specific responsibilities for the Department of Energy (DOE) Counterintelligence (CI) Program.

2. INQUIRIES . Inquiries concerning this Order should be directed to the Office of Counterintelligence, IN-20, U.S. Department of Energy, Washington, D.C. 20585, Telephone 202-586-7560.

3. /APPLICATION TO CONTRACTS. The provisions of this Order apply to all covered contractors to the extent implemented under a contract or other agreement. A covered contractor is a seller of supplies or services involving access to and protection of unclassified sensitive information, proprietary information, classified information, nuclear materials, or other safeguards and security interests under a procurement contract or subcontract.

4. REFERENCES. See Attachment 1.

5. DEFINITIONS. See Attachment 2.

6. POLICY. DOE'S policy is to develop a counterintelligence program in compliance with Executive Order 12333, 'United States Intelligence Activities" of 12-4-81 and such Executive orders as may supersede it, whose purpose to deter and neutralize foreign industrial or intelligence activities in the United States directed at or involving DOE programs, facilities, technology, personnel, unclassified sensitive information, and classified matter.

7. CONCEPT OF OPERATIONS.

   a. Each Headquarters and field element of the CI program will be designed to counter site-specific intelligence threats directed against its personnel, information, activities, facilities, and technologies.

   b. At Headquarters, the CI program will be implemented by the Office of Counterintelligence, IN-20.

DISTRIBUTION:
All Departmental Elements

INITIATED BY:
Office of Intelligence

c. In the DOE Field Offices, each Field Office Manager shall designate a Federal employee to serve as the Field Office CI Program Manager (CIPM). This program manager will have direct access to the Field Office Manager for sensitive CI activities and/or issues. The Counterintelligence Program Manager is authorized to conduct inquiries and administrative investigations including reviews of pertinent DOE information in the fulfillment of the CI mission. When an inquiry or administrative investigation provides reason to believe that there may be a basis for an espionage investigation, the matter will be immediately referred to the Federal Bureau of Investigation (FBI). This Order does not authorize any DOE or contractor employees to conduct espionage investigations or any other criminal investigations.

d. The Counterintelligence Program Manager will work with each DOE covered contractor to implement the CI program. Each DOE covered contractor, with the DOE concurrence and coordination, will designate a Contractor Counterintelligence Officer (CCIO) to assist in the implementation of the DOE Field Office CI program. The Contractor Counterintelligence Officer has authority to conduct preliminary inquiries and administrative investigations as described by the Field Office Counterintelligence Program Manager to assist in the fulfillment of DOE's responsibilities. The Contractor Counterintelligence Officer will have direct access to the DOE's Field Office Counterintelligence Program Manager and senior contractor management, on a need-to-know basis, for sensitive CI activities and issues.

8. RESPONSIBILITIES AND AUTHORITIES.

a. Director of Intelligence (IN-1) shall:

(1) Provide overall management of the CI program.

(2) Authorize all intelligence and counterintelligence activities within DOE conducted by authorized agencies of the intelligence community involving DOE resources including but not limited to personnel, facilities, technology, or materials.

(3) Recommend and promulgate all Departmental CI policy.

b. Director of Counterintelligence (IN-20) shall:

(1) Develop and implement methods, techniques, standards, and procedures for Departmental CI activities in accordance with applicable laws, regulations, intelligence procedures, and Departmental policies.

(2) Provide oversight for implementation of CI policy and procedures.

(3) Familiarize DOE CI personnel, including IN-20. DOE Field Office Counterintelligence Program Managers and Contractor Counterintelligence Officers, and other DOE employees working on CI, with the provisions of E.O. 12333 and other applicable policies and procedures.

(4) Establish a Headquarters (HQ) CI element to ensure compliance with applicable portions of this Counterintelligence Program Order.

(5) Support DOE Field Offices, in coordination with the responsible Program Secretarial Officer or Lead PSO, in the implementation of the Department's CI Program, and provide appropriate assistance in support of international treaty requirements and authorized intelligence community or law enforcement agency CI operations.

(6) Perform DOE national level liaison with authorized intelligence community or law enforcement agencies on CI matters. Review and approve all DOE CI field liaison with HQ elements of the intelligence community. This does not apply to activities of the Inspector General carried out pursuant to the Inspector General Act of 1978, as amended, 5 U.S.C. Appendix 3; Executive Order 12334; or other law, Executive order, Presidential directive, or regulation applicable to the Inspector General.

(7) Coordinate IN-1 approval for all CI activities and CI operations support requested by authorized officials of the intelligence community.

(8) Serve as the single DOE focal point for the CI program, represent DOE on national level CI committees, and coordinate CI interactions with other U.S. Government agencies.

(9) Manage the Departmental CI Analysis Program to advise DOE offices of the foreign intelligence threat. Conduct threat analysis, risk assessments, analytical studies, and identify assets, trends and patterns of foreign intelligence service activities directed against DOE.

(10) Implement the Department's CI Awareness Program. Ensure that the latest trends, patterns or threats of foreign intelligence service activities are incorporated in the Department's CI Awareness Program. Determine DOE's CI Awareness Program goals and coordinate with each DOE Field Office Counterintelligence Program Manager to ensure that CI awareness training objectives are met.

(11) Establish a CI briefing/debriefing program for foreign travel and contacts, and CI orientation briefings for new Federal and contractor employees.

(12) Monitor visits and assignments of foreign nationals to DOE facilities to assess relevant data pertaining to foreign intelligence service activities. Accomplish intelligence community indices checks (name traces) for all Departmental elements.

(13) Establish a format and reporting system for DOE Field Office Counterintelligence Program Managers to transmit CI information to DOE's Office of Counterintelligence (IN-20).

(14) Based on indicators of the existence or presence of espionage, conduct counterintelligence inquiries and administrative investigations.

(15) Provide appropriate support to intelligence operations approved by IN-1.

(16) Advise Office of Security Affairs (SA-1) and the cognizant PSO of CI investigations or inquiries into matters which might have a potential impact on DOE safeguards and security interests.

(17) Establish and maintain liaison with SA-1 and PSO's to facilitate the exchange and discussion of information regarding CI and/or safeguards and security related activities which may fall within the purview of both offices.

(18) Approve and issue Federal credentials and shields to designated CI personnel.

(19) Develop and implement a procedure to provide for independent oversight of the program as required by DOE 5630.12A.

c. Director of Security Affairs (SA-1) shall:

(1) Ensure policy is effected to support the Department's mission at both HQ and Field levels for coordination and exchange of information with IN-20.

(2) In accordance with applicable laws and regulations, establish policy and procedures for allowing access to all records maintained by the DOE complex to CI personnel at HQ and in the field when needed to perform their official duties.

(3) Ensure that any incidents or activities, involving a CI interest, identified within SA, especially within such programs as Technical Surveillance Countermeasures (TSCM), Operations Security (OPSEC), Computer (ADP) and Personnel Security, are properly coordinated with the DOE Office of Counterintelligence and the appropriate U.S. Government agencies.

(4) Perform DOE national level liaison with authorized U.S. Government agencies on Security Countermeasures (SCM) matters, to include but not limited to, TSCM, Physical Security, Personnel Security, OPSEC, and Unclassified and Classified Computer Security.

(5) Serve as the single DOE focal point for Security Countermeasures (SCM) programs, represent DOE on national level SCM committees, and coordinate SCM interaction with other U.S. Government agencies.

(6) Administer the program for the conduct of preliminary internal investigations of unlawful disclosures of classified information as specified in DOE 5631.5.

(7) Advise the Office of Intelligence (IN-1) of security investigations or inquiries into matters having a potential impact on DOE CI matters.

d. Program Secretarial Officers and comparable senior officials (includes the Assistant Secretaries for Conservation and Renewable Energy (CE), Defense Programs (DP), Fossil Energy (FE), Nuclear Energy (NE) , Environmental Restoration and Waste Management (EM), and the Directors of Energy Research, (ER), Civilian Radioactive Waste Management (RW), New Production Reactors (NP)), shall ensure implementation, by providing adequate financial and personnel resources, of an effective CI program at activities for which they exercise institutional oversight responsibilities.

e. Director of Naval Nuclear Propulsion Program (NE-60) shall, in accordance with the responsibilities and authorities assigned by Executive Order 12344 (statutorily prescribed by Public Law 98-525 (42 U.S.C. 7158, note)) and to ensure consistency throughout the joint Navy/DOE organization of the Naval Propulsion Program, implement and oversee all policy pertaining to CI activities under the Director's cognizance.

f. Managers of DOE Field Offices shall:

(1) Designate a Federal employee to serve as the CI Program Manager who will be the responsible Federal employee for implementing the CI program for the DOE Field Office and managing and administering local CI programs. The Counterintelligence Program Manager will have direct access to the Field Office Manager.

(2) Assure the implementation of the CI Program and applicable portions of this Order at all facilities under their control, including covered contractor and subcontractor locations.

(3) Ensure the CIPM receives ongoing CI training and sufficient updates necessary to satisfy requirements of this Order.

(4) Assure that Safeguards and Security field elements provide access to records including security and personnel security records as necessary for the CIPM to perform official duties. Develop standards for the protection of intelligence information developed from such records or security interviews in accordance with the Privacy Act and other applicable rules and regulations.

(5) Assure access to al 1 administrative records, including but not limited to computer, financial, personnel, and any other records necessary for the Field Office Counterintelligence Program Manager to perform official duties.

(6) Ensure that all Federal and contractor employees are aware of the requirement to report all contact with foreign nationals, and/or citizens of sensitive countries regarding sensitive subjects, classified information, or any CI related incidents, to include perceived efforts to obtain sensitive or proprietary data or other such attempts to obtain inappropriate cooperation. Additionally, all contacts with citizens of sensitive countries should be reported.

(7) Support all intelligence and CI efforts of other authorized agencies with investigative or collection jurisdiction over intelligence and CI activities, with concurrence of IN-1.

(8) Provide appropriate administrative and logistical support to the Field Office Counterintelligence Program Manager to allow for the successful 'implementation and conduct of the Field Office CI program.

g. Field Office Counterintelligence Program Managers shall:

(1) Ensure the development and imp lementation of a CI Program for DOE Field Offices, contractors, and subcontractors consistent with the intent of the Departmental CI Program.

(2) Develop and implement a CI Awa reness Program to meet CI program objectives in conjunction with the security education and awareness program.

(3) Perform liaison with authorized local intelligence community and law enforcement agencies on counterintelligence matters.

(4) Advise IN-20 of any specific CI educational requirements in conjunction with unique facility needs to ensure that specialized training curriculum may be tailored accordingly.

(5) Establish a system for limited CI incident examination, inquiries, resolutions, and/or referral to the appropriate Intelligence Community/law enforcement agency.

(6) Notify IN-20 within 24 hours of all incidents involving suspected or identified foreign intelligence activities and all incidents involving suspected or identified technical penetrations affecting persons or facilities under their jurisdiction.

(7) Coordinate with the Office of Safeguards and Security (SA-1O) to provide CI information for the foreign travel and contacts briefing program. Provide CI information for safeguards and security orientation briefings for new Federal and contractor employees.

(8) Establish and conduct a program for foreign travel and contacts debriefings.

(9) Establish a system to assure prompt transmittal of current CI threat information to contractor CI program designee.

h. Heads of Headquarters Elements and Field Organizations shall designate an individual(s) to be responsible for bringing to the attention of the contracting officer each procurement falling within the scope of this Directive. 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, “Request for Procurement").

i. Procurement Request Originators or such Other Individuals(s) (the individuals responsible for initiating a requirement on DOE F 4200.33) or such other individual(s) as designated by the cognizant head of headquarters element or field organization shall bring to the attention of the cognizant contracting officer the following: (1) each procurement requiring the application of this Directive, (2) requirements for flowdown of provisions of this Directive to any subcontract or sub-award, and (3) identification of the paragraphs or other portions of this Directive with which the awardee, or if different, a sub-awardee, is to comply.

j. Contracting Officers, based on advice received from the procurement request originator or other designated individual, shall apply applicable provisions of this Directive to awards falling within its scope. For awards, 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:

DOLORES L. ROZZI
Director of Administration
and Human Resource Management

REFERENCES.

1. Atomic Energy Act of 1954, which gives the Secretary of Energy the authority to protect against the disclosure of information that could adversely affect the health and safety of the public or the common defense and security of the United States.

2. Executive Order 12333, "U.S. Intelligence Activities," of 12-4-81, which sets forth the membership of the U.S. Intelligence Community and defines the duties, responsibilities, and general provisions for the conduct of intelligence/counterintelligence activities.

3. Executive Order 12334, "President's Intelligence Oversight Board," of 12-4-81, which sets forth requirements for the U.S. Intelligence Community reporting of intelligence activities.

4. National Security Decision Directive 44, "Organizing to Manage On-Site Verification of Nuclear Testing," of 7-90, which defines the duties and responsibilities of applicable agencies.

5. National Security Decision Directive 47, "Counterintelligence and Security Countermeasures," of 10-5-90, which establishes the U.S. counterintelligence goals for the 1990's.

6. National Security Decision Directive 197, "Reporting Hostile Contacts and Security Awareness," of 11-1-85, which establishes a requirement for each department or agency of the U.S. Government to establish formal awareness programs and procedures for reporting hostile contacts.

7. DOE 2320.1C, COOPERATION WITH THE OFFICE OF THE INSPECTOR GENERAL, of 5-18-92, which establishes Department of Energy policy for cooperation with the Office of Inspector General.

8. DOE 5630.12A, SAFEGUARDS AND SECURITY INSPECTION AND ASSESSMENT PROGRAM, of 6-23-92, which establishes an independent inspection and assessment program to determine the effectiveness of the Department's safeguards and security policies and procedures including their implementation across the Department.

9. 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.

10. DOE 5631.5, VIOLATIONS OF LAWS, LOSSES, AND INCIDENTS OF SECURITY CONCERNS, of 2-12-88, which addresses investigative authorities within the Department of Energy for violations of law.

DEFINITIONS.

1. COLLECTION.

   a. The exploitation of sources by collection agencies and the delivery of the information obtained to the appropriate processing unit for use in the production of intelligence.

   b. Obtaining information or intelligence information in any manner, including direct observation, liaison with official agencies, or solicitation from official, unofficial, or public sources.

   c. The act of employing instruments and/or equipment to obtain qualitative or quantitative data from the test or operations of foreign systems.

2. COUNTERINTELLIGENCE. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities, but not including personnel, physical, communications, or documents and other matter security programs.

3. ESPIONAGE. Overt, covert, or clandestine activity designed to obtain information relating to the national defense with intent or reason to believe that it will be used to the injury of the United States or to the advantage of a foreign nation.

4. FACILITY. An educational institution, manufacturing plant, laboratory, office building, or complex of buildings located on the same site that is operated and protected as one unit by the Department or its contractor(s).

5. HUMAN INTELLIGENCE (HUMINT). Intelligence information acquired by human sources through covert and overt collection techniques and open source data from foreign media.

6. INFORMATION. Unevaluated material of every description, at all levels of reliability, and from any source that may contain intelligence information.

7. INQUIRY. The collection and examination of information to include records review and interviews to assess indicators of espionage.

8. INVESTIGATION A comprehensive examination of facts or other pertinent information conducted by an authorized agency.

9. INTELLIGENCE. The product resulting from the collection, collation, evaluation, analysis, integration, and interpretation of all collected information.

10. INTELLIGENCE ACTIVITY. A generic term used to encompass any or all of the efforts and endeavors undertaken by intelligence organizations, including activities pursuant to collection, analysis, production, dissemination, and covert or clandestine activities. When used in the context of Executive Order 12333, the term intelligence activity means all activities that agencies within the Intelligence Community are authorized to conduct pursuant to Executive Order 12333.

11. INTELLIGENCE COMMUNITY AND AGENCIES WITHIN THE INTELLIGENCE COMMUNITY. A generic term defined in E.O. 12333 which refers to the following agencies or organizations:

a. The Central Intelligence Agency (CIA);

b. The National Security Agency (NSA);

c. The Defense Intelligence Agency (DIA);

d. The offices within the Department of Defense for the collection of specialized foreign intelligence through reconnaissance programs;

e. The Bureau of Intelligence and Research of the Department of State;

f. The intelligence elements of the Army, Navy, Air Force, and Marine Corps, the Federal Bureau of Investigation (FBI), the Department of the Treasury, and the Department of Energy;

g. The staff elements of the Director of Central Intelligence.

12. SECURITY COUNTERMEASURES. Defensive security programs and activities that seek to protect against both foreign intelligence collection efforts and unauthorized access to, or disclosure of, protected facilities, information, and material.