U.S. Department of Energy

Washington, D.C.

ORDER

DOE 5639.7

4-30-92

SUBJECT: OPERATIONS SECURITY PROGRAM

1. PURPOSE. To establish policies, responsibilities and authorities for implementing and sustaining the Department of Energy (DOE) Operations Security (OPSEC) Program.

2. CANCELLATION. DOE 5632.38, OPERATIONS SECURITY, of 1-29-88.

3. SCOPE. The provisions of this Order apply to all Departmental Elements.

4. APPLICATION TO CONTRACTS. The provisions of this Order are to be applied to covered contractors and they will apply 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 classified information, nuclear materials or other safeguards and security interests under a procurement contract or subcontract.

5. REFERENCES. See Attachment 1 for References.

6. DEFINITIONS. See Attachment 2 for Definitions.

7. POLICY. OPSEC techniques and measures shall be utilized throughout the Department to provide reasonable assurance that sensitive information and activities regarding national security and energy programs that could reveal program capabilities or intentions are protected from compromise and secured against unauthorized disclosure. The counterimagery program (CIP) shall be an integral part of the OPSEC Program pertaining to imagery-susceptible, sensitive activities.

8. RESPONSIBILITIES AND AUTHORITIES.

   a. The Secretary, through the Director of Security Affairs (SA-1) and the Director, Naval Nuclear Propulsion Program (NE-60), shall provide overall management of the OPSEC Program within DOE.

   b. Program and Staff Secretarial Officers shall:

      (1) Facilitate consistent OPSEC implementation within the Department.

         (a) Formally designate a representative and an alternate to the , Headquarters OPSEC Working Group.

DISTRIBUTION:

All Departmental Elements

INITIATED BY:

Office of Safeguards and Security

(b) Those designated should be from those assigned positions normally included in policy decisionmaking and who also have a routine interface with a broad range of other operational/policy areas of Headquarters.

(2) Ensure consistent OPSEC implementation throughout their respective organizations by such actions as:

(a) Monitoring the actions and products of field element OPSEC working groups and participating in these groups as appropriate.

(b) Reviewing and/or approving, as appropriate, OPSEC plans, the proposed threat statements, Critical and Sensitive Information Lists (CSIL) and supporting Essential Elements of Friendly Information (EEFI) for facilities under their programmatic responsibility.

(c) Providing support as required during conduct of OPSEC assessments, reviewing identified vulnerabilities, and making and/or approving recommendations for implementation of countermeasures and monitoring their effectiveness.

(3) Be provided advice and assistance through SA-10 related to the conduct of their respective OPSEC activities.

(4) Ensure an individual(s) is designated 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.

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

(1) Approve and promulgate Departmental OPSEC policy.

(2) Report annually, on December 1, to the Office of the Secretary on the status of the Department's Operations Security Program for the preceding fiscal year.

d. Director of Safeguards and Security (SA-10) shall:

(1) Provide the structure for implementation and coordination of the OPSEC program.

(2) Assess, analyze, evaluate, and develop overall OPSEC policy and standards.

(a) Appoint an OPSEC Program Manager who will be the primary point of contact for all Departmental OPSEC matters.

(b) Be advised of, review, and approve or disapprove, as appropriate, all DOE liaison with other Federal agencies and activities in the Washington, D.C. area on OPSEC matters. This does not apply to activities of the Inspector General, carried out pursuant to 5 U.S. C. App. 3 and Executive Order 12334.

(c) Publish an OPSEC procedural guide which provides guidance for use in conducting multidisciplinary OPSEC activities.

(d) Represent the Department at the national level on OPSEC related matters.

(e) Operate the Departmentwide office of record for OPSEC.

(3) Provide oversight responsibility for OPSEC policy.

(a) Establish a Departmental OPSEC Working Group to coordinate/assist the DOE OPSEC Program Manager, Headquarters OPSEC Manager, Headquarters program offices and field elements to ensure consistent OPSEC implementation Departmentwide.

(b) Assess the effectiveness of the Departmentwide OPSEC program by performing periodic OPSEC program reviews in coordination with the applicable program office(s).

(c) Coordinate with Headquarters program offices and field elements on OPSEC matters including the development of policies, standards, procedural guides, and other requirements which may impact their programs, and provide assistance as requested.

(d) Develop analytical tools to assist Headquarters program offices and field elements, as applicable, in the implementation of the Counterimagery program.

(4) Implement OPSEC policy at Headquarters.

(a) Institute and manage a DOE Headquarters OPSEC program as delineated in 8h.

(b) Plan and coordinate multidisciplinary support, including the conduct of OPSEC assessments and program reviews of selected Headquarters elements.

(c) Coordinate with the Office of Information Resources Management Policy, Plans, and Oversight (AD-24) on OPSEC assessments which include sensitive unclassified ADP activities and/or communications, transmission, or emission security activities.

(d) Analyze vulnerabilities detected in the course of Headquarters-sponsored assessments and recommend potential countermeasures as appropriate.

e. Director of Information Resources Management (AD-20) shall:

(1) Through AD-24:

(a) Represent DOE in matters concerning the unclassified computer security program.

(b) Review assessments and be aware of any unclassified computer security vulnerabilities detected in the course of an OPSEC assessment. Provide advice relative to the organizations responsible for correcting the vulnerabilities, when requested.

(c) Represent DOE in matters concerning communications security, transmission, and emission security.

(d) Assist in determining alternative solutions and courses of action to correct any telecommunications vulnerabilities detected in the course of an OPSEC assessment.

(2) Through the Director of Information Technology Services and Operations (AD-25):

(a) Review OPSEC assessments conducted at DOE Headquarters and be aware of any unclassified computer security vulnerabilities detected at Headquarters.

(b) Provide advice relative to the Headquarters elements responsible for correcting the vulnerabilities, when requested.

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

(1) Develop, in coordination with SA-10, Departmentwide guidelines, instructions, plans, and procedures on the protection of intelligence information within the Department.

(2) Coordinate with SA-10 to provide timely and current intelligence/threat information to support the OPSEC and counterimagery programs.

g. Director, Naval Nuclear Provision Program shall, in accordance with the responsibilities and authorities assigned by Executive Order 12344 (statutorily prescribed by 42 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 pertaining to this Order for activities under the Director's cognizance.

h. Managers of DOE Field Offices, Administrators of the Power Marketing Administrations and the Director of Safeguards and Security, for the organizations under their area of cognizance (SA-1O has the following responsibilities for Headquarters, and organizations not reporting through a DOE Field Office), shall:

(1) Institute, modify, and manage OPSEC programs and procedures at their respective locations and contractor facilities in accordance with this Order's policy statement and procedural guidelines; and, through their respective contracting officers, assure that contractors are required to comply with applicable provisions of this Order. This includes the identification of Class B and C facilities under their jurisdiction which warrant OPSEC protection and ensuring the implementation of an appropriate OPSEC program at such facilities.

(2) Establish a sufficient number of OPSEC working groups under the cognizance of each field element and at Headquarters, to perform the necessary management and support functions required for an effective OPSEC Program, to include OPSEC education and awareness. The working groups shall develop and set priorities for their OPSEC Program objectives consistent with approved plans and policies, meet on a regular basis, and maintain records of meeting, a copy of which shall be held by the responsible OPSEC Manager.

(3) Conduct OPSEC assessments of all Class A facilities falling within their purview. A copy of these assessments to include findings, recommendations, and actions taken will be provided to SA-10 for historical purposes.

(a) Either the programmatic or facility approach may be used to conduct the OPSEC assessment. If the facility approach is used, all activities at the facility will be included in the assessment. If the programmatic approach is used, all activities within the individual program will be included in the assessment.

(b) All Class A facilities which were not the subject of an OPSEC assessment under the requirements of DOE 5632.3B are required to have an assessment completed within 1 year of the effective date of this Order.

(c) Effective immediately, all Class A facilities are required to have an OPSEC assessment conducted at least every 2 years, or sooner if there are significant changes in the facility environment. If the programmatic approach is used and there is more than one major program located at the facility, a schedule will be developed and implemented which provides for the conduct of a minimum of one programmatic assessment annually. Major programs will be identified by the local OPSEC Working Group.

(4) Complete an initial OPSEC review of other sensitive activities and facilities within 1 year of the effective date of this Order, and conduct an OPSEC review whenever:

(a) New construction is planned that will process or store classified or sensitive information or material; or

(b) New sensitive activities are initiated or when significant changes occur to existing programs.

(5) Conduct OPSEC liaison with other field elements and local agencies. Advise SA-10 of broadly based OPSEC initiatives Involving these organizations.

(6) Ensure facilities included in the OPSEC Program develop and maintain OPSEC plans, procedures and program files to assist in implementing an active program, and approve these plans and procedures, as appropriate. OPSEC plans will include, at a minimum, goals, milestones, a timetable for accomplishing same, and, where applicable, an annex describing actions to identify and counter imagery collection from air- and space-borne platforms.

(7) Appoint an OPSEC Manager to implement the OPSEC program and ensure that OPSEC information promulgated by SA-10 is properly safeguarded and disseminated to authorized recipients.

(8) Ensure that OPSEC is addressed in safeguards and security planning and in Site Safeguards and Security Plans (SSSPs) and amendments, as appropriate.

(9) Analyze the results of OPSEC assessments and develop and implement countermeasures, as appropriate.

(10) Prepare a threat statement which describes the local OPSEC threat and develop a Critical and Sensitive Information List (CSIL) and supporting Essential Elements of Friendly Information (EEFI), which will be appropriately classified, set according to priorities, and disseminated to cognizant managers for review, comment and action based on the adequacy of countermeasures in place at each site. The threat statement and CSIL/EEFI will be reviewed by the cognizant OPSEC Working Group and senior Headquarters' program management and updated at least annually. The results of such reviews will be recorded in OPSEC Managers' files. Ensure that the periodic security surveys of facilities within the purview of the field element include a thorough Inspection of the OPSEC Program and an assessment of the practical impacts and effectiveness of the program.

(11) Conduct an initial review of all ongoing sensitive activities to identify those that are susceptible to imaging exploitation. Upon receipt of the multispectral imagery threat, the initial review will be refined for potential application of imagery countermeasures.

(12) Report annually, on November 1, to SA-10, and applicable program officials, on the status of their respective Operations Security programs for the preceding fiscal year.

(13) Ensure an individual(s) is designated 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.

i. Procurement request originators or such other individual(s) as designated by the cognizant Head of Departmental Elements shall bring to the attention of the cognizant contracting officer the following: (a) each procurement requiring the application of this Order; (b) requirements for flowdown of provisions of this Order to any subcontract or subaward; and (c) identification of the paragraphs or other portions of this Order with which the awardee, or, if different, a subawardee, 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 Order 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:

DONALD W. PEARMAN, JR.
Acting Director
Administration and Human
Resource Management

REFERENCES

1. Executive Order 12333, “United States Intelligence Activities, “ of 12-4-81, which describes the goals, direction, duties, and responsibilities of the national intelligence effort.

2. Executive Order 12334, “President’s Intelligence Oversight Board," of 12-4-81, as amended, which establishes the President’s Intelligence Oversight Board and prescribes its organization, duties, and responsibilities to enhance the security of the United States by ensuring the legality of activities of the intelligence community.

3. Executive Order 12344, “Naval Nuclear Propulsion Program,” of 2-1-82, as statutorily prescribed by PL 98-525 (42 USC 7158 note), which establishes the responsibilities and authority of the Director, Naval Nuclear Propulsion Program (who is also the Deputy Assistant Secretary for Naval Reactors within the Department) over all facilities and activities which comprise the joint Navy-DOE Program.

4. National Security Decision Order 298 entitled, “National Operations Security Program,” of 1-22-88, which describes the objective, process, policy and responsibilities to implement the national OPSEC program.

5. National Security Decision Order 309 entitled, ‘Nuclear Weapons Safety, Security, and Control,” of 6-27-88, and the National Security Advisor’s letter of 6-13-88, subject as above, which establishes steps to be taken to implement nuclear weapons safety and security and procedures to be followed in the annual reporting of the results of this effort.

6. DOE Operations Security Master Plan, of 1-1-91, which describes goals, directions, and milestones for implementing the OPSEC Program at Headquarters, DOE.

7. DOE Operations Security Procedural Guide, Volume I, Program/procedures, of 9-88, which establishes procedures for implementing this Order.

8. DOE 1240.2A, UNCLASSIFIED VISITS AND ASSIGNMENTS BY FOREIGN NATIONALS, of 1-19-89, which establishes the responsibilities, and policies and prescribes administrative procedures for visits and assignments by foreign nationals to DOE facilities for purposes involving unclassified matter.

9. DOE 1360.2A, UNCLASSIFIED COMPUTER SECURITY PROGRAM, of 5-20-88, which establishes requirements, policies, responsibilities, and procedures for developing, implementing, and sustaining a Department of Energy unclassified computer security program.

10. DOE 5300.1B, TELECOMMUNICATIONS, of 12-02-88, which establishes policy and general guidelines for using, reviewing, coordinating, and providing telecommunications service for Departmental Elements.

11. DOE 5300.2B, TELECOMMUNICATIONS: EMISSION SECURITY (TEMPEST) , of 5-22-86, which establishes the DOE telecommunications TEMPEST program for emission security and implements the provisions of the national policy applicable to emission security.

12. DOE 5300.3B, TELECOMMUNICATIONS; COMMUNICATIONS SECURITY, of 2-12-87, which establishes the DOE communications security program and implements the provision of the national policy applicable to communications security.

13. DOE 5630.8A, SAFEGUARDING OF NAVAL NUCLEAR PROPULSION INFORMATION (NNPI) , of 7-31-90, which defines NNPI and outlines disclosure policies and safeguarding requirements.

14* DOE 5630.11, SAFEGUARDS AND SECURITY PROGRAM, of 1-22-88, which establishes the policy and responsibilities for the Department of Energy Safeguards and Security Program.

15. DOE 5630.14, SAFEGUARDS AND SECURITY PROGRAM PLANNING, of 11-16-88, which establishes a standardized approach to protection program planning, and the responsibilities and authority for the process.

16. DOE 5631.2B, PERSONNEL SECURITY PROGRAM, of 5-18-88, which establishes the policy, responsibilities, and authorities for implementing the DOE personnel security program.

17. DOE 5632.1A, PROTECTION PROGRAM OPERATIONS, of 2-9-88, which establishes DOE policies for the physical protection of security interests and baseline physical protection standards.

18. DOE 5635.4, PROTECTION OF UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION (UCNI) , of 2-3-88, which delineates criteria for and protection of UCNI.

19. DOE 5636.3A, TECHNICAL SURVEILLANCE COUNTERMEASURES PROGRAM, of 2-3-88, which establishes procedures for implementing technical security programs.

20. DOE 5637.1, CLASSIFIED COMPUTER SECURITY PROGRAM, of 1-29-88, which establishes. uniform requirements, policy, responsibilities, and procedures for the development and implementation of Department of Energy classified computer security programs to ensure the security of classified information in automatic data processing (ADP) systems.

21. DOE 5670.1A, MANAGEMENT AND CONTROL OF FOREIGN INTELLIGENCE, of 1-15-92, which establishes requirements, policies, responsibilities, and procedures for the foreign intelligence activities of the Department of Energy.

22. Department of Energy Acquisition Regulation (DEAR) 970.5204-1 and 952.204-2, of 4-84, which specify the responsibilities of DOE contractors in protecting classified information.

23. Title 5 U.S.C. App. 3, The Inspector General Act of 1978, as amended, which describes the appointment, confirmation, duties, responsibilities and authorities of the Inspector General.

DEFINITIONS

1. Adversary. Any government, organization, group, or individual whose interests are inimical to those of the U.S. Government in general and to those of the Department in particular and that must be denied critical and sensitive information.

2. Counterimagery Program (CIP). A program designed to identify and counter the undesirable imagery collection potential of air- and space-borne platforms.

3. Critical and Sensitive Information List (CSIL) A list containing the most important aspects of a program or technology, whether classified or unclassified, requiring protection from adversary exploitation.

4. Essential Elements of Friendly Information (EEFI). Pathways or indicators in the form of data or activities that lead to specific Critical and Sensitive Information List items.

5. Field Elements. DOE or contractor facilities or activities located or conducted at sites outside the Metropolitan Washington, D.C., area.

6. Operations Security (OPSEC). A process designed to disrupt or defeat the ability of foreign intelligence or other adversaries to exploit sensitive Departmental activities or information and to prevent the unauthorized disclosure of such information.

7. OPSEC Assessment. An analysis of an organization or activity to identify information sources potentially exploitable by an adversary and the development of recommendations to mitigate these vulnerabilities.

8. OPSEC Manager. The individual designated by Headquarters, a field element, or a DOE contractor to be responsible for and provide direction to the DOE OPSEC program within their specific area of responsibility.

9. OPSEC Program Manager. The individual designated by the Director, Office of Safeguards and Security, to be the primary point of contact for the OPSEC Program and to serve as an interface for DOE with the national OPSEC community. The OPSEC Program Manager is responsible for and provides direction to the DOE OPSEC Program.

10. OPSEC Program Review (OPR). A formal review of subordinate OPSEC programs normally conducted by representatives of the Office of Safeguards and Security.

11. OPSEC Review. A broad scope review of a specific facility or activity to determine the level of OPSEC support required.

12. OPSEC Working Group. A formally designated body representing a broad range of administrative and programmatic activities at Headquarters, field elements, or contractor facilities which provides review, support, and participation with senior management in the implementation and furtherance of their OPSEC program.

13. Security Threat. The technical and operational capability of an adversary to detect and to exploit vulnerabilities.

14. Sensitive Activities. Classified or unclassified facilities, materials, programs, operations, inquiries, investigations, inspections, research, exercises, tests, training, and other functions of the Department or its contractors, which, if disclosed, could reasonably be expected to adversely affect national security interests.

15. Sensitive Information. Information the disclosure of which could reasonably be expected to adversely affect national or DOE security interests. This includes both classified and unclassified information and matter (e.g., Export Controlled Information, Naval Nuclear Propulsion Information, Unclassified Controlled Nuclear Information, Official Use Only information, and certain unclassified information, or matter) as identified in program Critical and Sensitive Information Lists.

16. Threat. The capability of an adversary coupled with his intentions to undertake any actions detrimental to the success of program activities or operation. (See Security Threat)