U.S. Department of Energy

Washington, D.C.

ORDER

DOE 5639.5

8-3-92

SUBJECT: TECHNICAL SURVEILLANCE COUNTERMEASURES PROGRAM

1. PURPOSE. To prescribe policies, responsibilities and authorities to establish the Department of Energy (DOE) Technical Surveillance Countermeasures (TSCM) Program. This Order implements the DOE TSCM Procedural Guide, DOE TSCM Operations Manual, DOE TSCM Report Writing Guide and Threat Assessment Scheduling System (TASS) which contain classified policies and procedures concerning the DOE TSCM Program.

2. CANCELLATION. DOE 5636.3A, TECHNICAL SURVEILLANCE COUNTERMEASURES PROGRAM, of 2-3-88.

3. 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 that is awarded a procurement contract or a subcontract involving access to classified information, special nuclear materials, unclassified sensitive information or other security interests.

4. EXCLUSION. DOE facilities and activities licensed by, or subject to licensing by the Nuclear Regulatory Commission (NRC) are exempt from the requirements of this Order. Office of Civilian Radioactive Waste Management (RW) personnel and activities not directly associated with the NRC licensed facilities and thus not covered by the Nuclear Regulatory directives are subject to the provisions of this Order.

5. REFERENCES. See Attachment 1 for References.

6. DEFINITIONS. See Attachment 2 for Definitions.

7. POLICY. The Department shall use technical surveillance countermeasures in conjunction with physical security, personnel security, communications security, and computer hardware, software and firmware security measures to protect classified information and other security interests in Department of Energy facilities or the facilities of its contractors. The Department of Energy TSCM Program shall be consistent with all Federal policies, procedures and standards. Application to the DOE TSCM Program is open to all minorities, women, and individuals who are physically and psychologically capable of performing the duties required by the DOE TSCM Program.

DISTRIBUTION:

All Departmental Elements

INITIATED BY:

Office of Safeguards and Security

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 TSCM Program within DOE.

b. Program Secretarial Officers (PSOs) shall:

(1) Provide line management oversight of TSCM programs and activities under their cognizance.

(2) Within one Year from the issuance of this Order, designate in writing a Federal employee who is formally trained in-all aspects of TSCM, to act as a-single point of contact to interface with the DOE TSCM Program Manager and all field elements under that PSO's control.

(3) Implement, for his or her organizational element, those portions of this Order applicable to Heads of Field Elements.

c. Director of Security Affairs (SA-1) shall recommend and promulgate Departmental TSCM policy.

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

(1) Provide the structure for implementation and coordination of the TSCM Program.

(2) Develop, analyze and implement TSCM policy and standards.

(3) Designate, in writing, a TSCM Program Manager who is a DOE Federal employee, formally trained in all aspects of the DOE TSCM Program, to manage and administer the Department's TSCM Program.

(4) Designate, in writing, two TSCM Field Coordinators who are DOE employees formally trained in TSCM operations and assigned to Field Operations Division (SA-13) to coordinate TSCM program activities with Field Elements.

(5) Implement, for Headquarters, those portions of this Order applicable to Heads of Field Elements and designate, in writing, a TSCM Operations Manager, who is a DOE employee formally trained in TSCM operations, to manage the Headquarters TSCM Program.

(6) Provide management support for the Technical Security Resource Center (TSRC) to serve as a clearing house for technical security information and to provide specialized TSCM research/development, training, and specialist testing for certification.

(7) Approve and issue credentials to TSCM Specialists who have been certified.

(8) Provide IN-40 all Sensitive Compartmented Information Facility (SCIF) related TSCM reports within 60 days of field surveys.

e. Director of Intelligence (IN-1): As the Department's Senior Intelligence Officer (SIO), grants final accreditation for all DOE Sensitive Compartmented Information Facilities (SCIFs) and shall:

(1) Request and coordinate requests for TSCM Services for SCIFs with the DOE TSCM Program Manager.

(2) Review reports of TSCM services rendered to SCIFs and monitor recommended corrective actions for identified technical/physical security findings, hazards, weaknesses and/or deficiencies.

(3) Provide SCI billets for DOE TSCM Specialists to insure that required TSCM services are completed as mandated by Director of Central Intelligence Directive (DCID) 1/22.

(4) Grants accreditation based on the results of a final TSCM Survey.

f. Director of Intelligence Support and Security (IN-40) shall:

(1) Request and coordinate TSCM Services for SCIF's with the DOE TSCM Program Manager.

(2) Review reports of TSCM services rendered to SCIF's and monitor recommended corrective actions to identified technical/physical security deficiencies, hazards, and/or weaknesses.

(3) Recommend to the SIO final SCIF accreditation, based on TSCM survey reports, which identify discrepancies, vulnerabilities, and risks.

g. Director of Information Resources Management (AD-20) through the Director of Information Resources Management Policy, Plans, and Oversight (AD-24) shall:

(1) Represent DOE in matters concerning the telecommunications security program.

(2) Review assessments and be aware of any telecommunications vulnerabilities detected in the course of a TSCM service. Provide advice relative to the organization's responsibility for correcting the vulnerabilities, when requested.

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

(4) Assist in determining alternative solutions and courses of action to correct any telecommunications vulnerabilities detected in the course of any TSCM service.

h. Director of 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 U.S.C. 7158, (note)) and to ensure consistency throughout the joint Navy/DOE organization of the Director, implement and oversee all policy pertaining to TSCM activities under the Director's cognizance.

i. Managers of DOE Field Offices. Heads of Field Elements, Administrators of the Power Marketing Administrations. and the Directors of Naval Nuclear Propulsion Program and Safeguards and Security, as appropriate, shall:

(1) Institute and manage the DOE TSCM program at their respective locations and contractor and subcontractor facilities in accordance with this Order's policy statement and procedural guidelines; and, through their respective contracting officers, assure that contractors comply with applicable provisions of this Order, the DOE TSCM Procedural Guide, and the DOE TSCM Operations Manual.

(2) Ensure that all facilities where classified information/material is discussed, processed, or manufactured are identified for TSCM services. All identified areas shall be analyzed and categorized in accordance with the Threat Assessment Scheduling System (TASS). All fiscal year scheduling of services shall be based upon TASS categorization. The acceptance of risk for any facilities that cannot receive the required TSCM services within the fiscal year shall be justified, in writing, and records maintained for a period of 3 years.

(3) Designate, in writing, a TSCM Operations Manager (TSCMOM), who is a DOE employee and who has demonstrated the skill and ability, either through experience or successful completion of a formal TSCMOM course of instruction, to successfully manage and administer the local DOE TSCM Program. This course of instruction will be provided by the Technical Security Resource Center (TSRC).

(4) Ensure that the TSCM Operations Manager receives adequate training and that ongoing proficiency training is maintained.

(5) 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 Form 4200.33, "Procurement Request Authorization").

j. DOE Technical Surveillance Countermeasures Program Manager shall:

(1) Ensure compliance with guidance and instructions provided in the DOE TSCM Procedural Guide and Operations Manual, which set forth the procedures for conducting the TSCM Program.

(2) Develop, acquire, and establish methods, techniques, standards, and procedures for TSCM activities.

(3) Direct required TSCM research and development efforts and assist in the acquisition of state-of-the-art TSCM equipment.

[4) Direct the operation of the Technical Security Resource Center (TSRC) in order to provide for the training, proficiency testing, and certification preparation of all DOE and DOE contractor TSCM Specialists.

(5) Ensure-that TSCM Operations Manager(s), TSCM Specialists and TSCM Officers are formally trained to perform their duties.

(6) Formally certify to the Director of Safeguards and Security, those DOE Contractor TSCM Specialists who are proficient in TSCM operations and activities.

(7) Assist the Office of Security Evaluations (EH-4) during the conduct of inspections/reviews of TSCM activities.

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

k. DOE TSCM Field Coordinators, in consonance with existing DOE policy and in coordination with the DOE TSCM Program Manager, shall:

(1) Coordinate and ensure compliance with DOE TSCM policies, standards, and procedures; review TSCM operations and inspection reports; and, provide for periodic onsite staff assistance visits to field organizations and contract programs.

(2) Provide advice and guidance to TSCM Operations Managers in administering the TSCM program to DOE or DOE contractor facilities.

l. Headquarters and Field Organization TSCM Operations Managers (TSCMOM) shall:

(1) Institute and manage TSCM programs at their respective locations using the DOE TSCM Procedural Guide for the conduct of TSCM activities. Enforce and ensure adherence to the protection standards contained in the DOE TSCM Procedural Guide and other interim policy documents as provided by the Director of Safeguards and Security.

(2) Evaluate and report on the effectiveness of those TSCM activities conducted at DOE and DOE contractor facilities under their cognizance at the end of each fiscal year. Copies of this report shall be provided to SA-10 through the Field Office Director of Safeguards and Security. Evaluations conducted as part of periodic safeguards and security inspections can serve as effective substitutions as long as they are accomplished on no less than an annual basis and are performed by the TSCMOM.

(3) Ensure that each DOE organization and DOE contractor organization designates, in writing, a TSCM Officer(s) as needed. The TSCM Officer(s) will be programmatically responsible to the TSCM Operations Manager as outlined in the DOE TSCM Procedural Guide.

(4) Disseminate to TSCM teams pertinent technical security information, including threat and hazard notices, approved equipment lists, updates to the DOE TSCM Procedural Guide, and local policy implementations.

(5) Develop supplemental directives which implement local TSCM policy. Local guidance will not be less stringent than DOE technical security requirements, and will clearly identify responsibilities and reporting requirements.

(6) Ensure that areas where classified information is discussed, processed, or manufactured on a recurring or routine basis receive TSCM services as categorized by the TASS results.

(7) Directs establishment of TSCM Teams by the appropriate contractor.

(8) Ensure that TSCM Specialists are trained at the Technical Security Resource Center and provided the opportunity to be certified by the DOE TSCM Program Manager.

(9) Ensure all TSCM activities are validated as required by the TSCM Procedural Guide and the TSCM Operations Manual, and approved in writing. Where time is a consideration, verbal tasking is authorized but written verification must be provided.

(10) Review and approve all TSCM Survey reports and ensure that all Findings are-forwarded to SA-13 for inclusion in the Safeguards and Security Issues Information System (SSIIS) Database.

(11) Ensure that all TSCM team managers and TSCM specialists receive applicable formal occupational health and safety training.

(12) Develop and implement a TSCM awareness and threat briefing program.

m. Procurement Request Originators or such other individuals(s) as designated by the cognizant head of the Headquarters or Field Element shall bring to the attention of the cognizant contracting officer the following: (1) each procurement requiring the application of this Order; (2) requirements for flowdown of provisions of this Order to any subcontract or subaward, and (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, 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.

o. Heads of Appropriate Departmental Elements shall require covered DOE contractors to develop, implement, and manage technical surveillance countermeasures programs in accordance with the provisions of this Order except paragraph 8a through 81.

p. Technical Surveillance Countermeasures Teams are responsible for providing TSCM services within the DOE community. TSCM Specialists assigned to these teams will be under the operational control of the cognizant TSCM Operations Manager. Note: Operational control equates to the TSCOMOM supervising and being responsible for the TSCM Specialists' actions regarding TSCM programmatic activities while contractor management will retain administrative control over TSCM Specialists and will not be accountable or liable for TSCM Specialists' actions other than those which fall under the area of administrative supervision. These teams shall:

(1) Perform TSCM surveys and inspections, upon request of the TSCMOM provide program awareness and threat briefings, provide preconstruction advice and assistance, and perform other TSCM activities as outlined in the DOE TSCM Procedural Guide or as assigned by the TSCM Operations Manager.

(2) Generate descriptive and detailed TSCM survey reports in accordance with the format and instructions contained in the TSCM Report Writing Guide.

(3) Receive applicable formal occupational health and safety training.

q. Technical Surveillance Countermeasures Officers (TSCMO) shall:

(1) Provide all necessary and required assistance to the TSCM teams to ensure that operations security and operational security requirements of the teams are met. This support is imperative to ensure that TSCM teams can accomplish the assigned mission within required and established guidelines. To avoid conflict of interest, the TSCM Officer will not exercise programmatic, managerial, or administrative control of the TSCM Teams.

(2) Certify to the TSCM Operations Manager that all new facilities identified for services are free of ongoing construction, are accessible and ready for TSCM services, and that these facilities have been constructed to meet the structural design requirements of DOE 6430.1A, GENERAL DESIGN CRITERIA, of 4-6-89 and the DOE TSCM Procedural Guide.

(3) Respond to, account for, and ensure adequate protection for all TSCM reports received from the TSCM team.

(4) Ensure that all physical and technical deficiencies or weaknesses identified by the TSCM team are properly addressed.

r. Manager of the Technical Security Resource Center shall:

(1) Provide TSCM training to DOE and DOE contractor personnel as directed by the DOE TSCM Program Manager.

(2) Collect, analyze, and disseminate technical security information, including threat hazard notices, approved equipment lists, and other pertinent TSCM information.

(3) Provide certification training for TSCM Specialists and assist the DOE TSCM Program Manager in conducting certification testing.

(4) Provide other services as directed by the DOE TSCM Program Manager.

BY ORDER OF THE SECRETARY OF ENERGY:

DOLORES L. ROZZI
Director of Administration
and Human Resource Management

REFERENCES

1. DOE 5300.1C, TELECOMMUNICATIONS, of 6-12-92, which establishes policy and general guidance for the use, review, coordination, and provision of telecommunications services for the Headquarters and field organizations.

2. DOE 5300.2D, TELECOMMUNICATIONS: EMISSION SECURITY (TEMPEST) , of 5-18-92, which establishes the telecommunications TEMPEST program for emission security and implements the provisions of the national policy that are applicable to emission security.

3. DOE 5300.4C, TELECOMMUNICATIONS: PROTECTED DISTRIBUTION SYSTEMS, of 5-18-92, which establishes policy and provides guidance concerning protected distribution systems used to transmit classified or sensitive unclassified information related to national security.

4. DOE 5631.5, VIOLATION OF LAWS, LOSSES, AND INCIDENTS OF SECURITY CONCERNS, of 2-12-88, which sets forth DOE procedures to assure timely and effective action relating to violations of criminal laws, losses, and incidents of security concern to DOE.

5. DOE 5632.6, PHYSICAL PROTECTION OF DOE PROPERTY AND UNCLASSIFIED FACILITIES, of 2-9-88, which establishes DOE policies and procedures for the physical protection of DOE property and unclassified facilities and to establish baseline physical protection requirements and standards for those interests.

6. DOE 5632.9, ISSUANCE, CONTROL, AND USE OF BADGES, PASSES, AND CREDENTIALS, of 2-3-88, which prescribes the policies and procedures for the issuance, control, and use of badges and passes which are used to control access to classified information and material.

7. DOE 5637.1, CLASSIFIED COMPUTER SECURITY PROGRAM, of 1-29-88, which establishes uniform requirements, policies, and responsibilities for the development and implementation of a program to ensure the security of information stored in classified automated data processing systems.

8. DOE 5639.7, OPERATIONS SECURITY PROGRAM, of 01-29-92, which establishes the DOE operations security program.

9. DOE 6430.1A, GENERAL DESIGN CRITERIA, of 4-6-89, which provides general design criteria (GDC) for use in the acquisition of the Department’s facilities and to establish responsibilities and authorities for the development and maintenance of these criteria.

10. DOE “Technical Surveillance Countermeasures Procedural Guide,” of 4-88, which establishes policy and procedures for the conduct and coordination of the DOE Technical Surveillance Countermeasures program.

11. DOE "Technical Surveillance Countermeasures Operations Manual," of April 1988, which provides procedures and methodology for the conduct of the DOE Technical Surveillance Countermeasures program.

12. DOE Threat Assessment and Scheduling System (TASS) User's Manual and Operating System, of May 1992, which describes the operation of the Threat Assessment and Scheduling System.

13. DOE 'Security Standards for Sensitive Compartmented Information and Facilities Procedural Guide," which implements guidelines governing the construction and protection of facilities for storing, processing, and the administrative handling of sensitive compartmented information.

14. CG-SS-2, "Classification Guide for Safeguards and Security Information," of July 1990, which provides classification determinations for National Security Information (NSI) concerning nuclear safeguards and various aspects of security and to provide guidance for derivatively classifying documents and materials containing such NSI, Restricted Data (RD), and Formerly Restricted Data (FRD).

15. Director of Central Intelligence Directive 1/22, "Technical Surveillance Countermeasures," of 7-3-85, which establishes policy and procedures for the conduct and coordination of technical surveillance countermeasures.

16. Director of Central Intelligence Directive Procedural Guides 1, 2, and 3, of 8-84, which set forth the procedures for the conduct of technical surveillance countermeasures services.

17. Executive Order 12333, 'U.S. Intelligence Activities," of 12-4-81, with classified attachment, which establishes policies and procedures for electronic surveillance (audio countermeasures) to determine the existence and capability of electronic surveillance equipment being used unlawfully.

18. Executive Order 12344, "Naval Nuclear Propulsion Program," of 2-1-82, as statutorily prescribed by Public Law 98-525 (42 U.S.C. 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.

DEFINITIONS

1. COMMUNICATIONS SECURITY (COMSEC). Measures and controls that deny information derived from telecommunications to unauthorized persons and ensure the authenticity of such telecommunications.

   NOTE: Communications security includes crypto security, transmission security, emission security, and physical security of COMSEC material.

2. COUNTERINTELLIGENCE. Intelligence activity intended to detect, counteract, and/or prevent espionage and other clandestine intelligence activities, sabotage, and international terrorist activities by or on behalf of foreign powers, organizations, or persons.

3. 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 contractors.

4. OPERATIONS SECURITY (OPSEC). A program 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.

5. SENIOR OFFICIAL OF THE INTELLIGENCE COMMUNITY. The senior official within a Department/Agency of the intelligence community charged with implementing Director of Central Intelligence policy and directives.

6. SENSITIVE COMPARTMENTED INFORMATION. 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.

7. SITE. A geographical area where one or more facilities are located.

8. TECHNICAL SECURITY. Includes TSCM, communications security, and the prevention or suppression of compromising emissions and emanations.

9. TECHNICAL SURVEILLANCE. The covert installation of devices or equipment to visually or audibly monitor activities within a target area to acquire information by technical means.

10. TECHNICAL SURVEILLANCE COUNTERMEASURES (TSCM). Systematic and effective measures for the detection and nullification of technical surveillance penetrations, technical surveillance hazards, and physical security weaknesses.

11. TEMPEST. Short name referring to investigation, study, and control of compromising emanations from telecommunications and automated information systems equipment.

12. THREAT ASSESSMENT SCHEDULING SYSTEM (TASS). A standardized system for identifying and prioritizing TSCM survey requirements (formerly Threat Assessment Procedure (TAP)).

U.S. Department of Energy

Washington, D.C.

PAGE CHANGE

DOE 5639.5 Chg 1

6-18-93

SUBJECT: TECHNICAL SURVEILLANCE COUNTERMEASURES PROGRAM

1. PURPOSE. To transmit revised pages to DOE 5639.5, TECHNICAL SURVEILLANCE COUNTERMEASURES PROGRAM, of 8-3-92.

2. EXPLANATION. This Page Change provides a corrected statement of Technical Surveillance Countermeasures Teams' roles and responsibilities and revised references which have been renumbered. Clarification is provided regarding operational control of specialists assigned to the teams and accountability for team members' actions. One new and three updated references are provided.

3. FILING INSTRUCTIONS.

a.

Remove Page	Dated	Insert Page	Dated
7	8-3-92	7	6-18-93
8	8-3-92	8	8-3-92
Attachment 1		Attachment 1	
Pages 1 and 2	8-3-92	Page 1	6-18-93
		Page 2	8-3-92

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

BY ORDER OF THE SECRETARY OF ENERGY:

LINDA G. SYE
Acting Assistant Secretary for
Human Resources and Administration

DISTRIBUTION:
All Departmental Elements

INITIATED BY:
Office of Intelligence
and National Security

(10) Review and approve all TSCM Survey reports and ensure that all findings are forwarded to SA-13 for inclusion in the Safeguards and Security Issues Information System (SSIIS) Database.

(11) Ensure that all TSCM team managers and TSCM specialists receive applicable formal occupational health and safety training.

(12) Develop and implement a TSCM awareness and threat briefing program.

m. Procurement Request Originators or such other individuals(s) as designated by the cognizant Head of the Headquarters or Field Element shall bring to the attention of the cognizant contracting officer the following: (1) each procurement requiring the application of this Order; (2) requirements for flowdown of provisions of this Order to any subcontract or subaward, and (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, 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.

o. Heads of Appropriate Departmental Elements shall require covered DOE contractors to develop, implement, and manage TSCM programs in accordance with the provisions of this Order except paragraphs 8a through 81.

p. Technical Surveillance Countermeasures Teams will assist the TSCM Operations Manager in carrying out TSCMOM programmatic oversight within the DOE community. TSCM specialists assigned to these teams will assist the cognizant TSCMOM and report directly to the TSCMOM for activities falling under the TSCM program. Note: The TSCMOM will have management, but not supervisory, control over TSCM specialist activities and functions arising under the TSCM program, in accordance with DOE 4200.3D, MANAGEMENT OF SUPPORT SERVICES CONTRACT ACTIVITY. These teams shall:

(1) Perform TSCM surveys and inspections, upon request of the TSCMOM, provide program awareness and threat briefings, provide preconstruction advice and assistance, and perform other TSCM activities as outlined in the DOE TSCM Procedural Guide or as assigned by the TSCMOM.

(2) Generate descriptive and detailed TSCM survey reports in accordance with the format and instructions contained in the TSCM Report Writing Guide.

(3) Receive applicable formal occupational health and safety training.

q. Technical Surveillance Countermeasures Officers (TSCMO) shall:

(1) Provide all necessary and required assistance to the TSCM teams to ensure that operations security and operational security requirements of the teams are met. This support is imperative to ensure that TSCM teams can accomplish the assigned mission within required and established guidelines. To avoid conflict of interest, the TSCM Officer will not exercise programmatic, managerial, or administrative control of the TSCM Teams.

(2) Certify to the TSCM Operations Manager that all new facilities identified for services are free of ongoing construction, are accessible and ready for TSCM services, and that these facilities have been constructed to meet the structural design requirements of DOE 6430.1A, GENERAL DESIGN CRITERIA, of 4-6-89 and the DOE TSCM Procedural Guide.

(3) Respond to, account for, and ensure adequate protection for all TSCM reports received from the TSCM team.

(4) Ensure that all physical and technical deficiencies or weaknesses identified by the TSCM team are properly addressed.

r. Manager of the Technical Security Resource Center shall:

(1) Provide TSCM training to DOE and DOE contractor personnel as directed by the DOE TSCM Program Manager.

(2) Collect, analyze, and disseminate technical security information, including threat hazard notices, approved equipment lists, and other pertinent TSCM information.

(3) Provide certification training for TSCM Specialists and assist the DOE TSCM Program Manager in conducting certification testing.

(4) Provide other services as directed by the DOE TSCM Program Manager.

BY ORDER OF THE SECRETARY OF ENERGY:

DOLORES L. ROZZI
Director of Administration
and Human Resource Management

REFERENCES

1. DOE 4200.3D, MANAGEMENT OF SUPPORT SERVICES CONTRACT ACTIVITY, of 8-31-92, which provides policy, procedures, and responsibilities for the management of support services contracts with the Department.

2. DOE 5300.1C, TELECOMMUNICATIONS, of 6-12-92, which establishes policy and general guidance for the use, review, coordination, and provision of telecommunications services for the Headquarters and field organizations.

3. DOE 5300.2D, TELECOMMUNICATIONS: EMISSION SECURITY (TEMPEST). of 5-18-92. which establishes the telecommunications TEMPEST program for emission security and implements the provisions of the national policy that are applicable to emission security.

4. DOE 5300.4C, TELECOMMUNICATIONS: PROTECTED DISTRIBUTION SYSTEMS, of 5-18-92, which establishes policy and provides guidance concerning protected distribution systems used to transmit classified or sensitive unclassified information related to national security.

5. DOE 5632.,6, PHYSICAL PROTECTION OF DOE PROPERTY AND UNCLASSIFIED FACILITIES, of 2-9-88, which establishes DOE policies and procedures for the physical protection of DOE property and unclassified facilities and establishes baseline physical protection requirements and standards for those interests.

6. DOE 5632.9A, ISSUANCE AND CONTROL, OF SECURITY BADGES, CREDENTIALS, AND SHIELDS, of 9-23-92, which prescribes the policies and procedures for the issuance, control, and use of badges, credentials and shields which are used to control access to classified information and material.

7. DOE 5639,3, VIOLATION OF LAWS, LOSSES, AND INCIDENTS OF SECURITY CONCERNS, of 9-15-92, which sets forth DOE procedures to assure timely and effective action relating to violations of criminal laws, losses, and incidents of security concern to DOE.

8. DOE 5639.6, CLASSIFIED COMPUTER SECURITY PROGRAM, of 9-15-92, which establishes uniform requirements, policies, and responsibilities for the development and implementation of a program to ensure the security of information stored in classified automated data processing systems.

9. DOE 5639.7, OPERATIONS SECURITY PROGRAM, of 1-29-92, which establishes the DOE Operations Security Pprogram.

10 . DOE 6430.1A, GENERAL DESIGN CRITERIA, of 4-6-89, which provides general design criteria for use in the acquisition of the Department’s facilities and to establish responsibilities and authorities for the development and maintenance of these criteria.

Vertical line denotes change.

11. DOE “Technical Surveillance Countermeasures Procedural Guide,” of 4-88. which establishes policy and procedures for the conduct and coordination of the DOE Technical Surveillance Countermeasures Program.

12. DOE “Technical Surveillance Countermeasures Report Writing Guide,” of 9-91, which standardizes correspondence and provides detailed guidance regarding TSCM reporting.

13. DOE “Technical Surveillance Countermeasures Operations Manual," of 4-88, which provides procedures and methodology for the conduct of the DOE Technical Surveillance Countermeasures program.

14. DOE “Threat Assessment and Scheduling System (TASS) User’s Manual and Operating System,” of 5-92, which describes the operation of TASS.

15. DOE “Security Standards for Sensitive Compartmented Information and Facilities Procedural Guide,” of 1-1-85, which implements guidelines governing the construction and protection of facilities for storing, processing, and the administrative handling of sensitive compartmented information.

16. CG-SS-2, “Classification Guide for Safeguards and Security Information," of 7-90, which provides classification determinations for National Security Information (NSI) concerning nuclear safeguards and various aspects of security and to provide guidance for derivatively classifying documents and materials containing such NSI, Restricted Data (RD), and Formerly Restricted Data (FRD).

17. Director of Central Intelligence Directive 1/22, “Technical Surveillance Countermeasures,” of 7-3-85, which establishes policy and procedures for the conduct and coordination of technical surveillance countermeasures.

18. Director of Central Intelligence Directive Procedural Guides 1, 2, and 3, of 8-84, which set forth the procedures for the conduct of technical surveillance countermeasures services.

19. Executive Order 12333, “U.S. Intelligence Activities,” of 12-4-81, with classified attachment, which establishes policies and procedures for electronic surveillance (audio countermeasures) to determine the existence and capability of electronic surveillance equipment being used unlawfully.

20. Executive Order 12344, “Naval Nuclear Propulsion Program," of 2-1-82, as statutorily prescribed by Public Law 98-525 (42 U.S.C. 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.