



**U.S. Department of  
Transportation**

Office of the Secretary  
of Transportation

**ORDER**

DOT 1650.1

12-8-93

Subject: TECHNICAL SECURITY COUNTERMEASURE PROGRAM

1. PURPOSE. This Order provides for the Department of Transportation (DOT) Technical Security Countermeasure (TSCM) Program, which reduces the threat to classified national security information from technical exploitation.
2. CANCELLATION. DOT 1600.16B, Technical Security Countermeasure Program, dated June 4, 1981.
3. SCOPE. The provisions of this Order apply to the Office of the Secretary (OST), the Operating Administrations (OAs) and the Bureau of Transportation Statistics (BTS).
4. REFERENCES.
  - a. Executive Order 12356, National Security Information, dated April 2, 1982.
  - b. National Communications Security Instruction (NACSI No. 4008), Safeguarding Communications Security (COMSEC) Facilities, dated March 4, 1983.
  - c. National Security Classification Guide (NSCG) HHB 70-9, dated August 1, 1982.
  - d. Director of Central Intelligence Directive (DCID) 1/21-1, Physical Security Standards for Sensitive Compartmented Information Facilities, dated September 1, 1987.
  - e. DOT 1600.17B, Use of Recording or Monitoring Equipment, Practices, and the Listening-in or Recording of Telephone Conversations, dated September 21, 1990.
  - f. Director of Central Intelligence Procedural Guide 1-2-3, dated August 1984.
  - g. DOT 1640.4C, Classification, Declassification, and Control of National Security Information, dated November 22, 1983.
5. DEFINITIONS.
  - a. TSCM Survey - is a complete electronic and physical examination of an area for the purpose of identifying technical surveillance devices or systems.

DISTRIBUTION: All Secretarial Offices  
All Operating Administrations  
Bureau of Transportation Statistics

OPI. Office of  
Security

- b. TSCM Inspection - is a noninstrumented inspection of an area to determine measures necessary to provide isolation or nullification of technical surveillance devices or systems.

6. BACKGROUND.

- a. Executive Order 12356, National Security Information, requires each department to set up measures that will prevent unauthorized persons from gaining access to classified national security information. Commercially available clandestine devices or systems provide techniques to gain such access. Foreign controlled intelligence collection efforts directed against the United States include the use of various technical devices. Hostile foreign or domestic criminal elements use devices that take many forms and employ various technologies and may use listening devices to monitor conversations in offices and conference rooms. They also use methods to attack telephones which, because of their extensive use in conducting business, are a continuous security hazard. Other devices may attack or alter information processing equipment, such as computers and printers which are especially vulnerable, and cause them to compromise the information being processed.

7. POLICY.

- a. Permanent communications security (COMSEC) facilities that process classified information will receive TSCM surveys and inspections that comply with NACSI No. 4008.
- b. Areas approved as Sensitive Compartmented Information Facilities (SCIF) will receive TSCM surveys and inspections that comply with DCID 1/21-1.
- c. COMSEC facilities and SCIFs shall be the only areas to receive TSCM surveys and inspections. Prior approval for exceptions must be granted by the Director, Office of Security (M-70), or for areas located within the Coast Guard, the Commandant (G-C).
- d. TSCM survey and inspection teams will consist of at least two people who have received appropriate Federal Government training.
- e. Because the United States Coast Guard (USCG) and the Federal Aviation Administration (FAA) have significant involvement in national defense and national internal security matters, both OAs will maintain a technical security countermeasure capability.

8. PROHIBITION AGAINST OFFENSIVE USE. DOT employees are prohibited from using clandestine listening or optical viewing devices, except for briefing and training under the TSCM program and while testing and maintaining countermeasure equipment. If devices are used in briefing and training, they must only show the general nature of the threat. The TSCM program is defensive in nature to detect the presence and prevent the introduction of clandestine listening devices. DOT 1600.17B outlines the authorized uses of listening, recording, or monitoring equipment.

9. RESPONSIBILITIES.

a. OST Office of Security (M-70) shall:

- (1) Issue departmental TSCM policies and the standards for TSCM equipment, survey and inspection techniques, and reporting, as well as standards for qualifications and level of competence for TSCM personnel.
- (2) Coordinate all aspects of the Department's TSCM program.
- (3) Represent DOT on Federal TSCM policy-making bodies.
- (4) Obtain assistance from other departments and agencies when appropriate.
- (5) Determine specific areas, including COMSEC facilities and SCIFs, that DOT TSCM teams must survey or inspect and the frequency of the surveys and inspections.
- (6) Establish and chair a DOT TSCM working group.

b. DOT TSCM Working Group will:

- (1) Consist of M-70 and those OAs with TSCM capability.
- (2) Evaluate the application and effectiveness of the department's TSCM inspection program.

c. USCG AND FAA. USCG and FAA shall each:

- (1) Maintain a TSCM program with survey and inspection capability in compliance with this Order.

- (2) Report to M-70:
    - (a) Six month schedules for surveys and inspections by October 1 and April 1 of each year.
    - (b) Non-COMSEC and non-SCIF inspections and surveys conducted or accomplished as authorized under Section 7.
    - (c) Inspection summary reports which provide the dates of inspections, describe what was inspected, list all hazards and findings, and outline required corrective actions. If corrective action is required, notify M-70 within 90 days after the date of the report. The notification shall show the corrective action taken by the DOT organization. Reports will be classified as outlined in Appendix A.
    - (d) When a listening device is found or if there is an indication that someone has introduced a device into an inspected area.
  - (3) Provide assistance and support to M-70, other departmental inspection teams, and other Government agencies when operationally possible. The USCG and FAA will coordinate these activities with M-70.
  - (4) May make routine contacts with the Federal Government's TSCM policy-making bodies and coordinate resulting significant developments with M-70.
10. DISCOVERY PROCEDURES. DOT cognizant security offices will develop discovery procedures which will comply with the Director of Central Intelligence Procedural Guide 1-2-3. Upon discovery of a suspected eavesdropping device, FAA and USCG shall adhere to their cognizant security offices' procedures for required actions. OST offices and all other OAs and BTS shall follow the procedures listed below.
- a. Take action to immediately secure the area. Upon discovery of a suspected eavesdropping device or system, the person or organization making the discovery shall not try to remove the device and must take action to secure the area to prevent the perpetrator from trying to remove the device. Discussions concerning the discovery or any classified or sensitive information must cease in the area.

- b. Make a report to M-70 using secure means. From a location other than the facility that contains the discovered device, the person or organization making the discovery will make a report to M-70. The report will be by secure means such as a Secure Telephone Unit (STU-III) or secure message to M-70 at FTS/commercial (202) 366-4677. If the DOT office does not have secure communications available another local Federal Government organization with such capabilities must be located. For discoveries made within the three DOT headquarters buildings, the report may be made in person by reporting to M-70, room 7402, 400 7th St., S.W., Washington, D.C. All information about the discovery of an eavesdropping device shall be classified as SECRET as outlined in Appendix A.
  - (1) Include the following information in the discovery report:
    - (a) Time, date, and specific location of discovery.
    - (b) Area, installation, and facility involved.
    - (c) Discovery method.
    - (d) Compromises, known or suspected, involving COMSEC facility operations or classified information.
- c. Continue to protect the suspected areas. The person or organization making the discovery will continue to protect the suspected area without compromising the situation while waiting for further instructions from M-70.
- d. Release of discovery information. Discovery information must be protected and released only to personnel with a need to know. If appropriate, M-70 shall inform the Federal Bureau of Investigation, the National Security Agency, and other counterintelligence organizations of the discovery.

11. REQUESTS FOR TSCM SERVICES.

- a. USCG and FAA shall submit requests for TSCM services to their cognizant security offices and follow organizational procedures for making such requests.
- b. All other Secretarial and OST offices, OAs and BTS shall follow the procedures outlined below.

- (1) Submit requests in writing. Requests for TSCM services must be submitted in writing to M-70 and must be classified SECRET to comply with National Security Classification Guide HHB 70-9, dated August 1, 1982.
  - (2) Include justification with identification of location. Requests shall include justification in compliance with paragraph 7 above and complete identification of the location to be inspected including street address, room number, type of facility and floor plans. It must also include a phone number of a STU-III where M-70 can contact the requesting party.
12. CONFIRMATION PROCEDURES. Inspection teams may issue confirmation of scheduled TSCM inspections either in writing via classified message or by using a STU-III. The notification will include instructions for the requesting organization including their providing details to the inspection team concerning administrative requirements such as door keys and secure equipment storage areas and instructions pertaining to the conduct and content of a briefing for employees who have a need to know about the TSCM survey.
13. OPERATIONS SECURITY (OPSEC). The success of a TSCM survey depends on the adherence to OPSEC procedures by the survey requester. Due to the possibility that someone may have compromised the facility by the installation of an eavesdropping device, there shall be no discussions concerning the TSCM inspection including the request, schedule, or TSCM team survey activities.

FOR THE SECRETARY OF TRANSPORTATION:



Paul T. Weiss  
For the Assistant Secretary  
for Administration

APPENDIX

SECURITY CLASSIFICATION AND DECLASSIFICATION GUIDE  
FOR TECHNICAL SECURITY COUNTERMEASURES (TSCM) PROGRAM

1. CLASSIFICATION AND DECLASSIFICATION. The classification and declassification criteria set forth below shall apply to all DOT material produced under the TSCM program. This Order shall be cited as the authority for the classification and declassification marking of material by DOT OAs except when material produced by DOT contains classified information about TSCM taken from or based upon a specific document from another department or agency. In that case the source document shall be respected and cited as the authority when marking the DOT material.
  - a. Classify correspondence identifying a location coupled with a date of a technical security survey as CONFIDENTIAL. Declassify 6 years from date of document.
  - b. Classify technical security survey reports, inspections, and technical summaries about technical surveillance hazards as CONFIDENTIAL. Declassify 6 years from the date of the document.
  - c. Classify information about hazards which survey teams cannot correct, that present a potential for continued exploitation, or that may exist in similar sensitive areas elsewhere as SECRET. Declassify 6 years from the date of the document. If the survey team later corrects the hazard or it no longer exists, they will change the documentation to CONFIDENTIAL and declassify 6 years from the date of the document.
  - d. Classify technical survey policies and procedures, criteria or limitations, of technical surveillance countermeasures equipment as SECRET. Declassify 6 years from the date of the document.

- e. Classify reports and correspondence that refer to the discovery of a clandestine device, or requests for TSCM services, as SECRET. All such correspondence shall be marked on the bottom portion of each page as follows:

"WARNING NOTICE: INTELLIGENCE SOURCES OR METHODS INVOLVED (WINTEL)"

Classified by: NSCG, HHB 70-9, of 8-1-82.  
Declassify on: OADR

Declassify 6 years from the date of the document. If a suspicious object is later identified as a technical surveillance hazard; then criterion b above would apply.

- f. Classified information furnished by a foreign government, in accordance with DOT 1640.4c, dated November 22, 1983, will be afforded the degree of protection equivalent to that required by the foreign classification markings. Unless otherwise directed by M-70, foreign government information shall not be assigned a date or event for declassification. Foreign government information is exempt from the declassification requirements prescribed for U.S. classified information.