U.S. Department of Transportation
Office of the Secretary of Transportation

ORDER

DOT 1600. 28

1-12-90

Subject: CONTROL OF COMPROMISING EMANATIONS

1. PURPOSE. This Order prescribes the Department of Transportation (DOT) policy and procedures for preventing the loss of classified information through compromising emanations.

2. SCOPE.

   a. All equipment and facilities (including automatic data processing (ADP), telecommunications, etc.) within DOT that process classified information are subject to the provisions of this policy.

   b. This policy is binding on all Secretarial Offices, Operating Administrations, and Contractors providing systems or facilities for DOT which handle classified information.

3. REFERENCES.

   a. National Telecommunications and Information Systems Security Policy (NTISSP) No. 300, National Policy on Control of Compromising Emanations, dated October 3, 1988.

   b. National Telecommunication and Information Systems Security Instruction (NTISSI) No. 7000, TEMPEST Countermeasures for Facilities, dated October 17, 1988.

   c. National Communications Security (COMSEC) Information Memoranda (NACSIM) 5100, Compromising Emanations Laboratory Test Requirements, Electromagnetic.

   d. Department of Transportation Computer Security (COMPUSEC) Program, DOT 1640.10, August 2, 1989.

4. BACKGROUND.

   a. It is the policy of the U.S. Government to prevent the loss of classified information through compromising emanations.

   b. Compromising emanations are defined as unintentional data-related or intelligence-bearing signals which, if intercepted and analyzed, disclose the classified information transmitted, received, handled, or otherwise processed by any information processing equipment. These phenomena are commonly known as TEMPEST.

c. The NTISSP No. 300, "National Policy on Control of Compromising Emanations," exists to prevent the loss of classified information through compromising emanations. It places the responsibility on the heads of departments and agencies to protect against the unintentional loss of classified information through the transmission of compromising emanations from equipment that is used to process classified information.

d. To achieve this objective, the effective edition of NACSIM 5100 was developed to provide compromising emanations requirements for new equipment/system development. In most cases within DOT, it will be possible to employ alternative methods that are reasonable, practical, and cost-effective to obtain TEMPEST security without requiring full NACSIM 5100 compliance.

e. NTISSI No. 7000 provides the measures and procedures for determining the TEMPEST countermeasure required for systems and facilities that process classified information within the U.S.

5. POLICY.

a. The procedures defined in NTISSI No. 7000 will be used within DOT by cognizant security offices (Attachment 1) to determine the TEMPEST countermeasures to be applied to equipment and facilities which process classified information.

b. No TEMPEST countermeasures are required for systems which will not be used to process classified information.

c. Based upon available TEMPEST threat and vulnerability assessment information and the recommendation of the cognizant security office, DOT elements shall select the appropriate emission security methods to protect its information processing equipment, systems, and facilities. The protection afforded the equipment, systems, and facilities must meet the standards set forth in the NTISSI No. 7000.

d. Prior to implementation, the OST Office of Security will review and approve:

(1) Level I TEMPEST countermeasures; or

(2) Level II TEMPEST countermeasures; or

(3) Level III thru V TEMPEST countermeasures which total more than $50,000 for a single Government facility or Government contractor facility; or

(4) Level III thru V TEMPEST countermeasures which total more than $50,000 of a contract's value.

6. RESPONSIBILITIES.

a. The Secretary of Transportation, through the Assistant Secretary for Administration, is responsible for planning, programming, implementing, and managing compromising emanations control programs to implement the provisions of the National Policy on Control of Compromising Emanations within the Department.

b. The Director, OST Office of Security, is the Executive Agent for the Assistant Secretary for Administration for the DOT TEMPEST program and is responsible for:

(1) Ascertaining the need for formulating and recommending Departmental TEMPEST policies, plans, and programs.

(2) Ensuring that planning, programming, and funding for implementing the compromising emanations control programs that comply with this Order and the provisions of the national policy are accomplished by the Secretarial Offices and the Operating Administrations.

(3) Appointing a Certified TEMPEST Technical Authority (CTTA), in accordance with reference 3b, to ensure that TEMPEST countermeasures incorporated at facilities and in equipment/system development programs are consistent with applicable national policy and instructions.

(4) Providing annually to the Countermeasures Advisory Panel (CAP) a current list of CTTAs acting on behalf of the Department.

(5) Providing annually to the Director, National Security Agency, any information related to the TEMPEST threat environment.

(6) Reviewing implementations that fall within the provisos of 5.d above.

(7) Reviewing and approving TEMPEST Orders that are drafted by Secretarial Offices and the Operating Administrations to implement this Order.

c. Cognizant Security Offices are responsible for:

(1) Contacting the Office of Security (M-70) as the focal point for questions and guidance concerning TEMPEST matters for computer security officers as described in the DOT 1640.10, Department of Transportation Computer Security (COMPUSEC) Program, dated August 2, 1989.

(2) Taking necessary measures to identify, prioritize, and correct compromising emanations from existing equipment, systems, and facilities that process classified information.

(3) Evaluating the need for TEMPEST countermeasures at the beginning of the procurement process for any information processing equipment that will be used for processing classified information.

(4) Evaluating equipment, systems, and facilities to determine the need for TEMPEST countermeasures and for conducting on-site evaluations of the effectiveness of those countermeasures.

(5) Establishing, as necessary, compromising emanations control measures during research, development, test, and evaluation (RDT&E) and procurement of new information processing equipment and systems that will be used to process classified information.

(6) Requiring contractors under DOT cognizance to comply with this policy.

(7) Promulgating to elements of DOT under their cognizance, the directives, standards, and instructions that will be necessary to implement the provisions of this policy.

(8) Requiring elements of DOT under their cognizance to coordinate their TEMPEST efforts in order to obtain support and avoid redundancy.

(9) Approving any and all TEMPEST requirements that are levied on DOT contractors.

(10) Obtaining the approval of the OST Office of Security for any TEMPEST countermeasures that fall within the provisos of 5.d. above.

d. Secretarial Offices and Operating Administrations of DOT are responsible for:

(1) Planning, programming, and implementing TEMPEST programs that comply with this policy for their areas of responsibility. They are also responsible for including in their budget submissions appropriate funding for these programs. This should begin with the FY-92 budget request.

(2) Having the procurement of any information processing equipment or systems that will process classified information evaluated and approved by the cognizant TEMPEST security office.

(3) Having any and all TEMPEST requirements that are to be levied on contractors approved by the cognizant security office.

e. Because of significant cost implications, compliance with this Order will be subject to review by the Office of Inspector General.

FOR THE SECRETARY OF TRANSPORTATION:

Melissa J. Allen
For the Assistant Secretary
for Administration

COGNIZANT TEMPEST SECURITY OFFICES

OPERATING ELEMENT	COGNIZANT SECURITY OFFICE
Office of the Secretary	Office of Security (M-70)
U.S. Coast Guard	Office of Command, Control and Communications G-TTS-4
Federal Aviation Administration	Program Engineering Service (APS-540)
Federal Highway Administration	Office of Security (M-70)
Federal Railroad Administration	Office of Security (M-70)
National Highway Traffic Safety Administration	Office of Security (M-70)
Urban Mass Transportation Administration	Office of Security (M-70)
St. Lawrence Seaway Development Corporation	Office of Security (M-70)
Maritime Administration	Office of Security (M-70)
Research and Special Programs Administration	Office of Security (M-70)