U.S. Department of Transportation

Office of the Secretary of Transportation

ORDER

DOT 1602.1

1-31-92

Subject: Department of Transportation Operations Security Program

1. **PURPOSE**. This Order establishes the Department of Transportation (DOT) Operations Security (OPSEC) Program, provides policy, assigns responsibility and implements National Security Decision Directive (NSDD) 298.

2. **SCOPE**.

   a. This Order applies to all Operating Administrations and Secretarial Offices of the Department assigned or supporting national security missions with classified or sensitive activities and/or strategic or other missions impacting national security.

   b. The DOT OPSEC Program shall be applied to DOT contractors when the DOT Operating Administrations and Secretarial Offices concerned have determined that such measures are necessary for the adequate protection of critical or sensitive information, activities or operations of the Department, directly or indirectly associated with a specific contract.

3. **REFERENCES**. National Security Decision Directive 298, "National Operations Security Program," January 22, 1988.

4. **BACKGROUND**.

   a. National Security Decision Directive 298 was signed by President Reagan in January 1988 and calls for each Executive Department and agency substantially involved in or supporting national security missions with classified or sensitive activities to establish a formal OPSEC program.

   b. Security programs and procedures already exist to protect classified matters. However, information generally available to the public as well as certain detectable activities reveal the existence of, and sometimes details about, classified or sensitive information or undertakings. Such indicators may assist those seeking to neutralize or exploit U.S. Government actions in the area of national security. Application of the OPSEC process promotes operational effectiveness by helping prevent the inadvertent compromise of sensitive or classified U.S. Government activities, capabilities, or intentions.

DISTRIBUTION: All Secretarial Offices
All Operating Administrations

OPI: Office of Security

c. The operations security process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures. The process begins with an examination of the totality of an activity to determine what exploitable but unclassified evidence of classified activity could be acquired in light of known collection capabilities of potential adversaries. Such evidence usually derives from openly available data. Certain indicators may be pieced together or interpreted to discern critical information. Indicators most often stem from the routine administrative, physical, or technical actions taken to prepare for or execute a plan or activity. Once identified, they are analyzed against the threat to determine the extent to which they may reveal critical information. Managers then use these threat and vulnerability analyses in risk assessments to assist in the selection and adoption of countermeasures.

5. **DEFINITIONS**.

a. Operations Security (OPSEC). A systematic and analytic process by which the U.S. Government and its supporting contractors can deny to potential adversaries information about capabilities and intentions by identifying, controlling, and protecting evidence of the planning and execution of sensitive activities and operations.

b. Critical Information. Information which must be protected from loss to keep an adversary from gaining a significant operational, economic, political, or technological advantage and prevent adverse impact on friendly mission accomplishment.

6. **POLICY**.

a. In accordance with NSDD 298 and paragraph 2, each Operating Administration and Secretarial Office to which this Order applies shall establish a formal OPSEC program.

b. In accordance with NSDD 298 and paragraph 2, those Operating Administrations and Secretarial Offices to which this Order applies and which have minimal activities that could affect national security need not establish a formal OPSEC program. However, they must cooperate with and support other departments, agencies, Operating Administrations, and Secretarial Offices to minimize damage to national security when OPSEC problems arise.

c. In accordance with NSDD 298 and paragraph 2, each Operating Administration and Secretarial Office to which this Order applies must address OPSEC from the beginning of all planning, programming and budgeting actions.

7. RESPONSIBILITIES.

a. The Assistant Secretary for Administration has Departmental responsibility for policies and procedures relating to the DOT OPSEC Program. The Assistant Secretary for Administration will provide Departmentwide guidance and assistance in OPSEC matters.

b. The Director, OST Office of Security, is the executive agent for the Assistant Secretary for Administration of the OPSEC Program. The Director is the DOT OPSEC Program Manager and shall:

(1) Develop department OPSEC policies, procedures, and planning guidance.

(2) Conduct an annual review of OPSEC procedures so as to assist in the improvement of OPSEC programs. Issue an annual call to the Operating Administrations and Secretarial Offices to submit a report of their annual reviews.

(3) Establish and chair a Departmentwide OPSEC working group to provide a forum to discuss generic and specific OPSEC problems in the Operating Administrations and Secretarial Offices.

(4) Coordinate OPSEC matters concerning more than one Operating Administration or Secretarial Office, as requested.

(5) Coordinate mutual support between an Operating Administration or Secretarial Office and other departments and agencies, as requested.

(6) Provide OPSEC planning, support, advice and training for Department headquarters senior officials and staff elements.

(7) Advise the National Security Council (NSC) on OPSEC measures required of other departments and agencies in order to achieve and maintain effective operations or activities within the Department.

(8) Delegate authority to plan, direct and implement OPSEC measures, as appropriate, to the Head of an Operating Administration and Secretarial Office.

c. Heads of each Operating Administration and Secretarial Office to which this order is made applicable under paragraph 2 above shall:

(1) Establish an OPSEC Program in accordance with the provisions of paragraph 6.a., above.

(2) Assign specific responsibility for OPSEC direction and implementation.

(3) Plan and implement specific OPSEC requirements in anticipation of and, where appropriate, during a qualifying activity.

(4) Use OPSEC analytical techniques to assist in identifying OPSEC vulnerabilities and to select appropriate OPSEC measures.

(5) Establish measures to ensure that all personnel, commensurate with their positions and security clearances, are aware of hostile intelligence threats and understand the OPSEC process.

(6) Establish requirements for an annual review and evaluation of OPSEC procedures to assist in the improvement of the OPSEC Program. Conduct an annual review and evaluation of the OPSEC Program to determine its effectiveness in the preceding year and to develop recommendations on improvements for the next year and the longer term. Upon request from the OST Office of Security, submit a report of these annual reviews to the Director, OST Office of Security through the Assistant Secretary for Administration, for review and approval. See Attachment 1 for guidelines concerning the annual report contents.

(7) Establish provisions for inter and intra-agency support and cooperation with respect to OPSEC programs.

(8) Support OPSEC programs and efforts by other Operating Administrations and Secretarial Offices and other government departments and agencies, as requested.

(9) Provide management, review, and inspection of their OPSEC Programs.

(10) Determine requirements for OPSEC measures by contractors. Ensure that these requirements are made known to the contractor as soon as possible and are incorporated specifically into requests for proposals and subsequent contractual documents in sufficient detail to enable cost estimates and compliance with OPSEC measures by contractors.

(11) Recommend to the Department's OPSEC Program Manager changes to policies, procedures, or practices to the DOT OPSEC Program.

(12) Develop OPSEC concepts and establish policies and procedures to supplement those developed by the Department OPSEC Program Manager, as necessary.

(13) Issue OPSEC planning guidance for activities of the Operating Administrations and Secretarial Offices, and for activities for which they have primary responsibility.

(14) Ensure adequate capabilities to execute OPSEC measures in support of Operating Administrations and Secretarial Offices activities.

(15) Designate an OPSEC Program Manager who will act as the focal point for OPSEC matters. The OPSEC Program Manager should receive appropriate formal OPSEC training.

(16) Inform the Director, OST Office of Security of OPSEC surveys that they conduct with other government departments and agencies. This should be done at the time of the OPSEC survey.

8. <u>IMPLEMENTATION</u>. Where appropriate, Secretarial Offices and/or Operating Administrations should develop additional guidance required to implement this Order and provide a copy of that guidance to the Office of Security, M-70, within six months of the date of the Order.

FOR THE SECRETARY OF TRANSPORTATION:

Paul T. Weiss
For the Assistant Secretary
for Administration

CONTENTS OF ANNUAL OPSEC REPORT

The annual report to the Director, OST Office of Security, should contain the following information:

1. The office name in the Operating Administration or the Secretarial Office which has responsibility for the OPSEC Program.

2. The name of the OPSEC Program Manager for the Operating Administration or the Secretarial Office.

3. The activities in the Operating Administration or the Secretarial Office to which OPSEC processes were applied.

   a. The critical information for each activity.

   b. The OPSEC vulnerabilities for each activity.

   c. The OPSEC measures taken for each activity.

4. The OPSEC awareness measures taken for each Operating Administration or Secretarial Office.

5. The effectiveness of the OPSEC Program for each Operating Administration or Secretarial Office. List the indicators that show this effectiveness.

6. Recommendations for improvement of the OPSEC Program for each Operating Administration or Secretarial Office.

7. The inter and intra-agency OPSEC support and coordination activities that each Operating Administration or Secretarial Office undertook.