U.S. Department of Transportation
Maritime Administration

MANUAL OF ORDERS

MARITIME ADMINISTRATIVE ORDER

| REVOKES | NO. |
|---|---|
| MAO 280-1 dtd. 5-17-84 | 280-1 |
| | EFFECTIVE DATE: January 7, 1992 |

SUBJECT

# SECURITY PROGRAM

## Section 1. Purpose:

This order provides for a security program designed to insure that all classified materials and restricted areas are provided adequate security protection while under the jurisdiction of the Maritime Administration.

## Section 2. Related Orders:

DOT 1600.17B Use of Recording or Monitoring Equipment, Practices, and the Listening-in or Recording of Telephone Conversations
DOT 1600.23 Demonstrations In or Near Government Buildings
DOT 1600.25 Consolidation of Physical Security Services for the DOT Washington Headquarters Facilities
DOT 1600.26A Department of Transportation Physical Security Program
DOT 1600.28 Control of Compromising Emanations
DOT 1610.2 National Communications Security Committee (NCSC) Policy and National Communications Security (COMSEC) Issuance System
DOT 1630.2A Department of Transportation Personnel Security Handbook
DOT 1630.3 Department of Transportation Personnel Security Policies
DOT 1640.2 Security for Electrically Transmitted Messages
DOT 1640.4C Classification, Declassification, and Control of National Security Information
DOT 1640.6 Office of the Secretary Procedures for Control of National Security Information
DOT 1640.9 Defensive Security Briefing Requirements for Departmental Personnel Traveling to Communist-Controlled Countries
DOT 1640.10 Department of Transportation Computer Security (COMPUSEC) Program
DOT 1660.5A Locking System for the Department of Transportation Headquarters (Nassif) Building
DOT 1660.6A Reporting Procedures for Incidents Occurring Within the Department of Transportation Headquarters Facilities

## Section 3. Policy:

Each employee of the Maritime Administration granted clearance for access to classified security information shall become familiar with and follow the detailed instructions applicable to the classification, safekeeping, reproduction, distribution, and destruction of classified materials, and for the security protection of offices and restricted areas; the provisions of this order; supplemental instructions as may be issued by the Maritime Administration Security Officer; and the directives referenced in section 2.

Section 4. Responsibilities:

4.01 The Security Officer shall be responsible to the Associate Administrator for Administration for the installation of the security program of the Maritime Administration, and the enforcement of security policies, regulations, and procedures in consonance with the security regulations of the Department of Transportation. The Security Officer shall:

1 Be responsible for the receipt, custody, transmission, and control of all materials classified TOP SECRET or SECRET with the exception of the physical custody of such material as is authorized under the provisions of section 8.03 of this order.

2 Prepare instructions, within the framework of established policy and regulations, for the guidance of Assistant Security Officers and other personnel.

3 Make periodic inspections to insure that adequate and proper security precautions are taken to safeguard restricted areas and classified and controlled information at all times.

4 Recommend designations of classifying and declassifying officers, designate messengers who may be permitted to carry classified materials, and designate employees who may authorize release of classified materials to persons outside of the Federal Government.

5 Maintain and publish current listings of persons for whom security clearances have been obtained.

6 Maintain liaison with the Office of Security, Department of Transportation, on security matters.

4.02 The Deputy Security Officers shall be responsible to the Security Officer and assist in the administration of the security program. The Deputies, as appropriate, shall act as the Security Officer when that official is absent or unable to serve.

4.03 Associate Administrators, Office Directors, Region Directors, and the Superintendent, U. S. Merchant Marine Academy, are responsible for all aspects of physical and personnel security in their area of jurisdiction. These officials shall designate an Assistant Security Officer and an alternate Assistant Security Officer for their immediate area of jurisdiction, and for such offices as Reserve Fleets and Construction Representatives. Such designations shall be reported in writing to the Security Officer. The Security Officer shall serve as Assistant Security Officer for the Offices of the Maritime Administrator, Deputy Administrators, and the Secretary.

4.04 Assistant Security Officers shall be responsible for the security program within their organizational unit. Specifically, they shall:

1 Be assured that all employees who require access to classified materials in the performance of their routine or emergency duties have been issued access authorizations and are given adequate instructions in the security regulations and procedures.

2 Promptly report loss or compromise of classified materials and any other security violations to the Security Officer.

3 Furnish to the Security Officer a list of representatives of other agencies or organizations who have been invited to attend special conferences or committee meetings in which classified information may be involved, sufficiently in advance to permit the Security Officer to request the required security clearance. Exception: This requirement shall not apply to routine contacts or meetings, provided the Assistant Security Officer has been notified by the other government agency that the employee involved has the required security clearance.

4 Install an adequate system of inspection to insure full compliance with personnel and physical security policies, regulations, and procedures.

5 Maintain an inventory of all classified material in the unit.

6 Establish procedures to ensure that all material, safes, and safe files within their jurisdiction are secured at the end of each workday. Maintain a "Security Container Check List" form SF 702 for each safe and safe file.

4.05 Employees shall comply with all personnel and physical security directives and safeguard all classified information, materials, and documents, in accordance with the security classification assigned and the directives cited in section 2 of this order. These materials and documents will be properly stored for safekeeping in an authorized container at the end of each workday.

Section 5. Personnel Security:

5.01 It shall be the responsibility of Associate Administrators, Office Directors, Region Directors, or the Superintendent, U. S. Merchant Marine Academy, to specify the sensitivity of each position on form SF 52, "Request for Personnel Action," in block "3." If the position is designated as either a critical sensitive or a noncritical sensitive position, there shall also be indicated in the "Remarks" section the degree of classified information or material to which the incumbent will have access. Designations of sensitive positions, as defined in DOT 1630.2A, shall be kept to the minimum required.

5.02 Before a Maritime Administration employee is assigned or appointed to any sensitive position, an access authorization shall be obtained as follows:

1 Assistant Security Officers shall submit a form DOT F 1600.8, "Personnel Security Action Request and Notification," in triplicate, to the Personnel Officer in Washington, D.C. In the field this form shall be submitted by or via the appropriate Personnel Representative.

2 Each request must be accompanied by those forms required by DOT 1630.2A for the type of clearance desired, and by the employee's official personnel folder. For new government employees not having a personnel folder, an up-to-date form SF 171, "Application for Employment," should be included. Where the official employee folders are filed in Headquarters Office of Personnel, that office will attach the folder to the request.

3 After review and the signature of the Personnel Officer, the Office of Personnel shall transmit the documents to the Security Officer for concurrence and for submission to the Office of Security, Department of Transportation.

4 Upon issuance of a security certification by the Office of Security:

(1) The Security Officer shall advise the Assistant Security Officer of the clearance granted. The form DOT F 1600.8 reflecting the clearance will be filed by the Security Officer, and a copy will be filed in the employee's official personnel folder by the Office of Personnel.

(2) After a security briefing, a form SF 312, "Classified Information Nondisclosure Agreement," shall be properly executed before the Security Officer in Washington, D.C., or an Assistant Security Officer or alternate in the field. The original shall be forwarded for file in the Office of Security, Department of Transportation.

5.03 A certificate of security clearance which is issued for a specific purpose or event, or for a specific period, shall be valid only for the purpose, event, or period indicated. Certificates issued for incumbents of sensitive positions shall be effective until revoked. Revocation shall be made by special notice to the individual, and deletion from the next published master list of persons with a security clearance.

5.04 Persons whose services are procured by contract which will require the contractor to have access to classified information or material shall be cleared in advance through the Security Officer. A security clearance should also be requested in cases where the program official or the contracting officer deems it prudent.

5.05 Special security clearance procedures are also available for nonemployees such as National Defense Executive Reservists, Ships' Masters and Radio Officers, Union and Shipyard Officers, and Members of the Defense Shipping Council (Formerly Defense Shipping Executive Board). Security clearances are also obtained for employees and nonemployees requiring access to NATO and cryptographic material.

5.06 When an employee having a security clearance is leaving the Maritime Administration or no longer requires a clearance, the employee will be debriefed by the Security Officer, or Assistant Security Officer at field installations.

Section 6. Classification Authorities:

6.01 Original classification authority within the Maritime Administration is limited to the following officials and levels of classification. No official within this agency has authority for original classification at the TOP SECRET level.

1 SECRET and lower - Maritime Administrator/Director,
National Shipping Authority

2 CONFIDENTIAL - Associate Administrator for Policy and
International Affairs
Director, Office of International Activities
Director, Office of National Security Plans

6.02 Derivative classification authority within the Maritime Administration, for material classified TOP SECRET or lower, is limited to the following officials:

Maritime Administrator/Director, National Shipping Authority
Deputy Maritime Administrators
Associate Administrator for Policy and International Affairs
Director, Office of International Activities
Director, Office of National Security Plans
Region Directors
Superintendent, U.S. Merchant Marine Academy

6.03 Effective upon declaration of civil readiness level INITIAL ALERT or the comparable military readiness level, both original classification authority for SECRET or lower and derivative classification authority for material TOP SECRET or lower is assigned to the following officials. This special authority is automatically terminated when both civil and military readiness levels return to the level of COMMUNICATIONS WATCH or comparable readiness state.

Deputy Maritime Administrators
Associate Administrator for Policy and International Affairs

Director, Office of International Activities
Director, Office of National Security Plans
Region Directors
Superintendent, U.S. Merchant Marine Academy
Heads of ALFA, BRAVO, and CHARLIE Emergency Teams, if activated.

6.04 Authorities listed in 6.01, 6.02, and 6.03 above may not be redelegated but may be exercised by persons authorized in writing to act for designated officials during their absence.

6.05 Classifying officials shall report original and derivative classification actions in accordance with requirements established by the Security Officer.

Section 7. Declassification/Downgrading Authorities and Procedures:

7.01 The following officials, in addition to the classifying officers listed in section 6.01 of this order, are authorized to declassify or downgrade classified information and material in their functional areas which information was originally classified by an official of this or one of its predecessor agencies. This authority may not be redelegated but may be exercised by persons authorized in writing to act for designated officials in their absence.

Deputy Maritime Administrators
Chief Counsel
Security Officer
Associate Administrator for Administration
Associate Administrator for Maritime Aids
Associate Administrator for Shipbuilding and Ship Operations
Associate Administrator for Marketing
North Atlantic Region Director
Central Region Director
Western Region Director
South Atlantic Region Director
Great Lakes Region Director
Superintendent, U.S. Merchant Marine Academy

7.02 Declassification/Downgrading Authorities, in addition to the duties prescribed in Chapter III, DOT 1640.4C, shall:

1 Act upon requests originating within the Maritime Administration for the declassification or downgrading of classified material. In every instance the appropriate notation (as described in DOT 1640.4C) will be used to record a change in classification, as appropriate.

2 Notify holders of documents when action to declassify or downgrade the material is different than that contained in or on the document (e.g., declassification before an automatic downgrading date).

3 Notify the Security Officer of downgrading or declassification of all documents, whether automatic or otherwise.

7.03 It has been determined that all material originally classified by the Maritime Administration or its predecessor agencies that is dated prior to December 31, 1959, is declassified.

7.04 Requests received from outside agencies or departments for Maritime Administration concurrence in changing classification of classified material originating within the Maritime Administration shall be directed to the Security Officer for the coordination of the request with interested offices and the preparation of replies.

Section 8. Document Security:

8.01 Only incumbents of sensitive positions for whom access authorizations have been obtained shall, within the limit of the security clearance specified and their "need-to-know," be authorized to have access to classified information, materials, and documents.

8.02 Classified materials may be delivered by messengers who have been granted security clearances to carry such materials. This clearance will not authorize a messenger to have access to the contents of the material. Messengers are not authorized to carry information or material classified TOP SECRET.

8.03 No Maritime Administration organization element shall maintain custody of material classified SECRET or TOP SECRET without the written authorization of the Security Officer. Where such authority is granted, the Assistant Security Officer shall be accountable to the Security Officer for the proper discharge of the custodial responsibility.

8.04 Reproduction of classified documents or materials, at self-service copier stations or otherwise, must have prior approval of the Security Officer. Where reproduction is authorized, copies will be assigned the same control number and further annotated with copy numbers as prescribed by the Security Officer. Caution should be exercised to be certain all papers are removed from the copier and surrounding area and all scrap copies are destroyed as prescribed in section 9 of this order.

Section 9. Document Destruction:

9.01 Maritime Administrative Order 250-3, "Records Management Program," defines record and nonrecord material; related questions shall be referred to the Records Management Officer. Nonrecord and record material authorized for disposition in either the General Records Schedules or the MARAD Records Control Schedule may be destroyed when no longer required in accordance with the following instructions:

1 For material marked SECRET or NATO SECRET, a form DOT F 1600.22, "Destruction of Classified Records," shall be prepared by the Assistant Security Officer in triplicate and delivered to the Security Officer with the material or documents to be destroyed. Separate forms shall be submitted for SECRET vs. NATO SECRET. The Security Officer shall receive the material, and return an annotated copy of the receipt to the Assistant Security Officer. The annotated receipt will be the basis for deleting the destroyed material from the active inventory; and receipts will be retained until after completion and approval of the annual inventory.

2 In Washington, D.C., CONFIDENTIAL, NATO CONFIDENTIAL, LIMITED OFFICIAL USE material, and Privacy Act material will be placed in destruction bags obtained from the Security Officer. (These bags are numbered; no other type bag may be used for this purpose.) After removal of all staples, paper clips, and other metallic fasteners, and placement of the material in the bag, the bag will be stapled closed. Arrangement for pickup may be made by calling the Correspondence Branch on Mondays to schedule a Tuesday pickup. Material disposed of using this procedure shall be deleted from active inventories.

3 In field activities, each Assistant Security Officer is responsible for establishing an effective destruction mechanism for CONFIDENTIAL, NATO CONFIDENTIAL, LIMITED OFFICIAL USE, and Privacy Act material.

4 Material marked "FOR OFFICIAL USE ONLY" may be destroyed by tearing it into small pieces and assimilating it with a sufficiently large volume of other waste material to preclude reconstruction.

Section 10. Physical Security:

10.01 The following listed facilities are considered susceptible to covert actions, which could result in hazards such as disturbances, sabotage, pilferage, or access to classified, sensitive, or privacy act data, and they are therefore designated as restricted areas. To the degree required for each, facility managers are responsible for providing adequate physical security to preclude unauthorized entry, ensuring that personnel given access have appropriate levels of security clearance when required, and providing for escorts or employee monitoring of visitors.

National Defense Reserve Fleets
MARAD Operations Center
Headquarters Telecommunications Center
Headquarters Office of Personnel
Division of Accounting Operations
Firefighting Schools
ADP Terminal Areas

USMMA - Student Record Areas
Outported Ready Reserve Force Ships

10.02 Reporting of Suspected Thefts of Government or Personal Property:

A Maritime Administration employee discovering the theft of government or private property shall immediately report the incident to the activity's Personal Property Management Officer who shall take action in accordance with current property management regulations and shall subsequently report such incidents to the Maritime Administration Security Officer. This procedure is part of the Maritime Administration Incident Reporting Program (See Appendix).

Section 11. Emergency Protection Procedures:

11.01 Assistant Security Officers for the following facilities are responsible for developing a plan for the protection, removal, or destruction of classified material in case of fire, natural disaster, civil disturbance, or enemy action in the event of war. Such plans will be coordinated with and are subject to the approval of the Security Officer.

Headquarters Telecommunications Center
MARAD Operations Center
National Defense Reserve Fleets
Region Headquarters, Field Offices and Outported Ready Reserve Force Ships
Ship Construction Field Offices

11.02 The Security Officer shall develop and disseminate, as appropriate, an emergency plan for the protection, removal or destruction of classified material located at headquarters.

11.03 Any employee planning travel outside the Continental United States with classified material of any nature shall be briefed by the Security Officer or an Assistant Security Officer on emergency destruction procedures prior to departure on travel.

11.04 Priorities for emergency destruction shall be based on the degree of classification, then types of material within each classification. Emergency destruction priorities are 1) TOP SECRET, 2) SECRET, and 3) CONFIDENTIAL in descending order; within each classification the order of destruction is 1) COMSEC material, 2) special access material, and 3) all other material, to include NATO. Additional guidance is available to holders of COMSEC and NATO material in NACSI No. 4010, "Routine Destruction and Emergency Protection of COMSEC Material" and USSAN Instruction 1-69, respectively. In all instances of the destruction of COMSEC material, the instructions in NACSI No. 4010 prevail.

11.05 Where classified material other than COMSEC is to be destroyed, and depending on the location, the following methods shall be considered as alternatives to regularly available destruction devices:

1 Jettison at sea at depths of 1,000 fathoms or more - If that water depth is not available, and time does not permit other emergency destruction, the material will, nonetheless, be jettisoned to prevent its easy capture. When shipboard emergency destruction plans include jettisoning, weighted bags shall be made available. If a vessel is to be sunk through intentional scuttling or is sinking due to hostile action, classified material will be locked in security filing cabinets or vaults and allowed to sink with the vessel rather than attempting jettisoning.

2 Dismantle or smash metallic items beyond reconstruction, by available means such as sledgehammers, cutting tools, torches, etc.

3 Use disposal equipment not normally associated with the destruction of classified material, such as garbage grinders, sewage treatment plants, and boilers.

4 Douse the classified material with a flammable liquid and ignite it, when no other method can be employed.

11.06 Assistant Security Officers shall report to the Security Officer by the most expeditious means when emergency protection plans have been implemented. Such reports will include actions taken, identification of all classified material destroyed and method of destruction, and any material not destroyed and presumed to have fallen into unauthorized hands.

Section 12. Communications Security:

All aspects of Communications Security (COMSEC) are discussed in various issuances from the Director, National Security Agency (NSA) as defined in DOT 1610.2. Caution must be exercised to never discuss classified matter over an unsecured telephone (this includes FTS), or to send any sensitive material over an unsecured facsimile device or computer/electronic mail network. Similar precautions should be taken to avoid discussion over a telephone of unclassified "national security related" material which could be useful to an adversary.

Earnest Hawkins

EARNEST HAWKINS
Associate Administrator
for Administration

MARITIME ADMINISTRATION INCIDENT REPORTING PROGRAM

1. INCIDENT REPORTING. An incident reporting program is an essential element in any security program. It is not enough to develop a comprehensive set of security controls for a facility without being concerned about the loss/theft or malicious damage (including arson) of Maritime Administration (MARAD) property. One test of how effectively the security controls are working is the number and type of security incidents that occur at a facility.

2. REPORTING REQUIREMENTS. The timely reporting of thefts, losses or malicious damage of MARAD property to the appropriate security element is imperative. The quicker the incident report is made, the greater the possibility of recovering the property and apprehending the perpetrator. In addition to the timeliness of the reports, they must be accurate and complete, especially in the description of the property involved and the circumstances surrounding the incident. What is done with the report after it is received by the Security Officer or the Assistant Security Officers is also a good measurement of the program's effectiveness. If the reports are not analyzed or acted upon in a prompt, decisive manner, the reporting and control systems are undermined.

3. INDIVIDUAL RESPONSIBILITIES. An employee discovering the theft or malicious damage or loss of MARAD property has an obligation to report the discovery immediately, in person or by telephone (followed by a written report), to the cognizant Security Officer or Assistant Security Officer. Those officials will determine the extent of additional reporting required, e.g., to the Federal Bureau of Investigation (FBI), local law enforcement agencies, building security, etc. In the event there is no local MARAD servicing security element, contact the appropriate Assistant Security Officer for the Region or field unit for that organization. (For employees assigned to the DOT Headquarters facilities, the reporting procedures set forth in the DOT 1660.6A apply.) It should be noted that the channels for reporting missing or stolen Government-owned property by property custodians under the property management regulations do not supplant the requirement to report such matters to the security element. However, through local arrangements between the security and property management offices, reporting procedures can be developed that would satisfy both the property control and security requirements. Form MA-925, Report of Survey, should be used to report in writing theft or damage to Government-owned property.

4. RESPONSIBILITIES OF THE SERVICING SECURITY ELEMENT.

   a. Maintain contact with local FBI offices and local law enforcement agencies to determine the criteria and procedures for reporting thefts of Government-owned property to those elements for action/investigation.

b. Upon receiving a report involving the loss/theft or malicious damage of Government property, the servicing security element should:

(1) Determine the accuracy and completeness of the information, insuring that it presents as complete a picture as possible of what happened, when and where and who or what may have been responsible for the incident.

(2) Determine whether the FBI and/or the local law enforcement agency should be or have been notified of the incident.

(3) Initiate, if appropriate, an investigation of the incident, including, if need be, an on-site visit where the incident occurred. This decision should be based on the following:

- Is this an isolated incident or one of a series of such incidents which may indicate a possible pattern?
- Does the stolen, lost or damaged property have a high-dollar value or importance to the mission of the facility?
- Is it the type of stolen property that could be readily converted to personal use or sold illegally; for example, a typewriter versus a specialized piece of test equipment?
- Does the description of the circumstances surrounding the incident reveal a possible weakness or void in the security controls at the facility? If the facility had not been previously surveyed or inspected, the reported incident could provide the basis for scheduling a visit in the immediate future.
- Advise the designated headquarters office by the most expeditious means available if the incident is of such gravity or importance as to warrant alerting the headquarters; for example, the destruction by arson of an entire facility and its contents or the wholesale theft of office equipment from a particular facility. For other than unusual incident reports, security field elements should submit summary reports to their headquarters office on a regularly scheduled basis, categorizing the security incidents that occurred within the established reporting period.