DOT ORDER AND MANUAL 1640.4E

CLASSIFIED NATIONAL SECURITY INFORMATION

Office of the Secretary

Office of the Assistant Secretary for Administration

Office of Security

Table of Contents

DOT ORDER AND MANUAL 1640.4E, Classified National Security Information

DOT Order 1640.4E

I. Purpose 1

II. Background 1

III. Cancellations 1

IV. References 2

V. Policy 2

VI. Applicability 2

VII. Delegated Program Authority 3

VIII. Responsibilities 3

IX. Implementation 7

DOT Manual 1640.4E

Chapter 1. General Information 1-1

1-1. Purpose 1-1

1-2. References 1-1

1-3. Classified Information Explained 1-1

Chapter 2. Methods of Classifying Information 2-1

2-1. Derivative Classification 2-1

2-2. Original Classification 2-1

2-3. Duration of Classification 2-2

2-4. Reducing the Volume of Classified Documents 2-2

Chapter 3. Individual Responsibilities 3-1

3-1. Responsibility to Protect Classified Information 3-1

3-2. Sharing/Disclosure of Classified Information 3-1

3-3. Protecting Classified Information 3-1
3-4. Reporting of Loss, Compromise, or Unauthorized Disclosure 3-1
Chapter 4. Classification Challenges 4-1
4-1. Challenging Classification 4-1
4-2. Procedures 4-1
4-3. Agency Response 4-1
4-4. Appeals 4-2
4-5. Departmental Information Security Review Committee 4-2
4-6. Other Considerations 4-2
Chapter 5. Marking 5-1
5-1. Classification Marking for Paper Documents 5-1
5-2. Classification Marking for Electronic Documents 5-1
5-3. Portion Marking 5-2
5-4. Marking Originally Classified Documents 5-2
5-5. Marking Derivatively Classified Documents 5-2
5-6. Marking Transmittal Documents 5-5
5-7. Marking of Foreign Government Information 5-5
5-8. Marking of Working Papers 5-5
5-9. Marking Classified Equipment and Bulky Material 5-6
5-10. Unmarked Materials 5-6
5-11. Compilations 5-6
5-12. Commingling of Restricted Data (RD) and Formerly Restricted Data (FRD) with Information Classified Under E.O. 13526 5-7
5-13. Classification Marking in the Electronic Environment 5-7
Chapter 6. Declassification 6-1
6-1. Automatic Declassification 6-1
6-2. Systematic Declassification Review 6-6
6-3. Declassification Guides 6-6
6-4. Mandatory Review for Declassification 6-7
6-5. Referrals 6-9
6-6. Discretionary Declassification 6-11

6-7. Classified Information in the Custody of Private Organizations or Individuals 6-11
6-8. Assistance to the Department of State 6-11
Chapter 7. Safeguarding 7-1
7-1. General 7-1
7-2. Security Containers 7-1
7-3. Open Storage Areas and Vaults 7-3
7-4. Cover Sheets 7-3
7-5. Burn Bags 7-3
7-6. Destruction 7-3
Chapter 8. Storage 8-1
8-1. Levels of Protection 8-1
8-2. Foreign Government and NATO Information 8-2
Chapter 9. Reproduction and Electronic Processing of Classified Information 9-1
9-1. Reproduction 9-1
9-2. Electronic Processing 9-1
9-3. Electronic Storage Media 9-1
Chapter 10. Transmission and Transporting: Sending and Receiving Classified Documents and Material 10-1
10-1. General 10-1
10-2. Packaging of Classified Documents and Equipment 10-1
10-3. Control Points 10-2
10-4. Inventory of Classified Information 10-2
10-5 Carrying Classified Information 10-2
10-6 Couriers and Courier Letters 10-3
10-7. Transmission Methods Within and Between the U.S., Puerto Rico, or a U.S. Possession or Trust Territory 10-3
10-8. Transmission Methods to a U.S. Government Facility Located Outside the U.S. 10-4
10-9. Transmission of U.S. Classified Information to Foreign Governments 10-4
10-10. Electronic Transmission of Classified Information 10-4
Chapter 11. Other Requirements 11-1
11-1. Self Inspection Program 11-1

11-2. Security Education Program 11-1
11-3. Reports 11-1
11-4. Decommissioning of Classified Storage and Information Processing Equipment ... 11-2
11-5. Departure from DOT Components 11-2
Appendix 1: Guidance for Original and Derivative Classification Authorities A1-1
Appendix 2: Using Secure Telephones A2-1
Appendix 3: Classified Discussions A3-1
Appendix 4: Forms and Labels for Controlling and Protecting Classified Information A4-1
Appendix 5: Inquiries and Investigations Concerning Possible Loss, Compromise, or Unauthorized Disclosure of Classified Information A5-1
Appendix 6: Photocopying Classified Information A6-1
Appendix 7: Transporting Classified Information Overseas A7-1
Appendix 8: Restricted Data and Formerly Restricted Data A8-1
Appendix 9: Technical Security A9-1
Appendix 10: Critical Element for Managing Classified Information A10-1
Appendix 11: Classification and Declassification Guides A11-1
Appendix 12: Glossary/Definitions A12-1

Department of Transportation
Office of the Secretary of Transportation

ORDER

1640.4E

January 21, 2011

Subject: CLASSIFIED NATIONAL SECURITY INFORMATION

I. PURPOSE: This order contains policies and assigns responsibilities for the classification, declassification, and control of national security information throughout the Department of Transportation (DOT). It implements Executive Order (E.O.) 13526, Classified National Security Information.

II. BACKGROUND: The Information Security Oversight Office (ISOO) has implemented E.O. 13526 through Title 32, Code of Federal Regulations (CFR), Part 2001, Classified National Security Information, which applies to all Executive Branch agencies. This DOT Order 1640.4E implements the policies and procedures set forth in E.O. 13526 and in 32 CFR Part 2001.

III. CANCELLATIONS.

1. This Order cancels the following publications:

(a) DOT Order 1640.4D, Classified Information Security Management, dated December 9, 1997;

(b) DOT Manual 1640.4D, Classified Information Security Management, dated December 9, 1997, except for Chapter 5, For Official Use Only Information, which remains in effect until a new order addresses that subject;

(c) DOT Security Bulletin 00-04, dated December 19, 2000. This bulletin is incorporated into Appendix 6, Photocopying Classified Information.

(d) DOT Security Bulletin 00-1, dated February 22, 2002. This bulletin is incorporated into Appendix 5 of Inquiries and Investigations Concerning Possible Loss, Compromise, or Unauthorized Disclosure of Classified Information.

2. The following publications were cancelled by an earlier version of this Order and are listed here for informational purposes:

(a) DOT Order 1640.1, Control and Protection of "For Official Use Only" Information, dated December 27, 1971.

(b) DOT Order 1640.2, Security for Electrically Transmitted Messages, dated June 14, 1972.

(c) DOT Order 1640.4C, Classification, Declassification, and Control of National Security Information, dated November 11, 1983.

(d) DOT Security Bulletin 96-01, Implementing Instructions for Executive Order 12958, Classified National Security Information, dated April 17, 1996.

IV. REFERENCES:

1. Presidential Order of December 29, 2009, Original Classification Authority.

2. Executive Order (E.O.) 13526, Classified National Security Information.

3. Title 32, Code of Federal Regulations, Part 2001, (32 CFR Part 2001), National Archives and Records Administration, Information Security Oversight Office (ISOO).

4. E.O. 12968, Access to Classified Information.

5. 49 CFR Part 8, Classified Information: Classification/Declassification/Access.

6. DOT Manual 1640.4E, Guide for Managing Classified Information (published in conjunction with this Order), hereafter referred to as the Manual.

V. POLICY:

1. It is DOT policy to ensure that all classified national security information is properly protected. DOT information relating to the national security shall be uniformly classified, protected, and declassified pursuant to all classified national security information security statutes, Executive Orders, and regulations.

2. It is DOT policy to ensure that the public has access to as much DOT information as possible, consistent with the need to protect the national security and other concerns such as privacy, security, proprietary business interests, and law enforcement investigations.

3. Users of this Order shall refer concurrently to E.O. 13526 and 32 CFR Part 2001 (i.e., national security policy) for guidance. In the event of a conflict between this Order and national security policy, national policy takes precedence. Users should report conflicts to the Director, Office of Security (M-40).

VI. APPLICABILITY:

1. This Order applies only to information that is classified in accordance with Executive Order 13526 or any successor thereto. Other types of sensitive information such as "For Official Use Only" and "Sensitive Security Information" are addressed in other DOT Orders and correspondence from the Assistant Secretary for Administration and/or the Director of Security, M-40.

2. This Order applies to all DOT components, and to all DOT Federal employees, detailees, contractor employees, or other persons employed or contracted to perform work for DOT (subsequently identified as employees and contractors) who receive, store, process, generate, discuss or otherwise handle classified information or have the potential to handle classified information.

VII. DELEGATED PROGRAM AUTHORITY:

The Federal Aviation Administration (FAA) is delegated the authority to administer its own classified national security information management program under the oversight of M-40. The FAA may adopt procedures that implement DOT classified national security information policies in ways different from those prescribed in this order and appendices, consistent with Executive Orders, directives and federal regulations.

VIII. RESPONSIBILITIES:

1. The Assistant Secretary for Administration (M-1), as the Senior Agency Official for classification management in accordance with 49 CFR Part 8 shall:

(a) direct and administer the DOT classification management program;

(b) issue DOT-wide policy to ensure effective compliance with and implementation of relevant Federal statutes, Executive Orders, and regulations, including those listed in REFERENCES above;

(c) represent DOT with respect to other agencies and organizations both within and outside the Federal Government, on classified information management policy and issues;

(d) periodically evaluate DOT's implementation of and adherence to classification management policies and requirements;

(e) provide through the Director, Office of Security, M-40, classification management support services for the Office of the Secretary (OST) and for those DOT components that have not been delegated their own classification management authority;

(f) as required, prepare consolidated classification management program reports for and on behalf of DOT; and

(g) chair the Information Security Review Committee (described in 49 CFR 8.9), which decides upon issues and challenges regarding the management of classified information in DOT.

2. Original Classification Authorities shall:

(a) receive initial and annual training in proper classification (including the avoidance of over-classification) and declassification as provided in E.O. 13526.[1]

(b) be able to support any classification decisions that they make, including identifying or describing the damage, should the classification decision become the subject of a challenge or access demand pursuant to Executive Order 13526 or other law.[2]

---

[1] Failure to take initial and annual training shall result in the withdrawal of classification authority until the training is completed (Section 1.3(d), E.O.13526).

[2] There is no requirement, at the time of the decision, for the original classification authority to prepare a written description of such damage. However, the original classification authority must be able to support the decision in writing if necessary, and may want to prepare separate documentation for future reference.

(c) ensure that any original classification decisions that they make are incorporated into a classification guide as soon as practicable.

3. Secretarial Officers and Heads of Operating Administrations shall:

(a) implement policies promulgated by the Assistant Secretary for Administration and ensure that all provisions are effectively administered;

(b) ensure that every DOT Federal employee, contractor employee, or any other person employed or contracted to perform work for DOT is aware that markings other than "Top Secret," "Secret," or "Confidential" shall not be used to identify classified national security information;

(c) prepare and submit all required reports;

(d) provide personnel and funding for the proper safeguarding, classification, and declassification activities required by this Order;

(e) ensure that declassification reviews of archived information are conducted on a regular basis;

(f) promptly take any corrective actions that may be warranted;

(g) ensure that the performance standards of all employees and contractors whose duties significantly involve the creation, handling, or management of classified information include the management of classified information as a critical element to be evaluated in their ratings;[3]

(h) appoint security officers or security points of contact for classified information management to assist M-40 in implementing DOT's classified information management program within their components and to represent their component; and provide a list of the appointed individuals to M-40, annually, as personnel change, or as otherwise required by M-40;

(i) ensure that organizational emergency contingency plans include provisions for the proper transportation, handling, storage, and destruction of any classified information that may be necessary during an emergency; and

(j) ensure that security infractions and violations involving classified information are reported to their servicing security organizations, as well as any information that might reflect adversely upon an individual's suitability for a security clearance.

4. The Director, Office of Security, M-40, shall:

(a) provide guidance and direction throughout DOT on all classification management matters;

[3] Appendix 10 contains an example of a critical element regarding the management of classified information.

(b) provide classified information security support services for OST and for those DOT components that have not been delegated their own information security management authority;

(c) provide active oversight[4] and continuing security education and awareness programs to ensure effective implementation of security policies and requirements;

(d) authorize exceptions to DOT classification management policies and procedures when doing so meets an urgent management need, is consistent with the interests of national security, does not infringe on the rights of any individual, and does not conflict with authority reserved to either the Secretary or the Assistant Secretary for Administration;

(e) relay to DOT components requests and requirements as they are received from ISOO and respond to ISOO with consolidated reports for DOT; and

(f) provide liaison with other Federal Government agencies as needed on classification management matters and represent DOT on committees and working groups within and outside the Federal Government regarding classified information security management.

5. Security Officers and Security Points of Contacts (excluding FAA) shall:

(a) serve as a liaison between their components and M-40 regarding all matters relating to classification and the protection of classified information;

(b) assist in establishing and maintaining visit control procedures for situations in which visitors to their component are authorized access to classified information;

(c) serve as their component's focal point for the reporting of possible security violations, compromises, or other threats to the safeguarding of classified information, in accordance with 32 CFR 2001.48 and Appendix 5 to the Manual, Inquiries and Investigations Concerning Possible Loss, Compromise, or Unauthorized Disclosure of Classified Information.

(d) assist the Office of Security, M-40, in performing the following services for their administration or office:

(1) implementing the component's classified information security management program;

(2) advising their component head on matters related to the classification, downgrading, declassification, and safeguarding of national security information;

(3) implementing an effective security education program as required by Chapter 11 of the Manual and by 32 CFR 2001.70 and 2001.71;

---

[4] Includes oversight authority over all DOT organizations, including any organization with delegated authority to administer its own classified information program.

(4) establishing procedures for ensuring that all individuals handling classified information are properly cleared;

(5) as necessary, ensuring that classification guides and/or declassification guides for classified plans, programs, and projects are distributed and maintained;

(6) periodically reviewing classified documents that are originally classified by their component to ensure that classification decisions are appropriate, and ensuring that documents containing other agencies' equities are referred to those agencies for review before the documents are released;

(7) ensuring that declassification reviews of information that is originally classified by their components are conducted on a regular basis, both of archived information and of information in current files; prepare declassification plans, or submit information to M-40 regarding the status of declassification activities of the component;

(8) consistent with operational and statutory requirements, conducting a continuous review of classified documents in coordination with the component's Records Management Officer; and, through declassification, destruction, or retirement of records, reducing to the extent possible the amount of classified information the component maintains;

(9) submitting periodic reports as required by 32 CFR 2001.90, Statistical Reporting, and Chapter 11 of the Manual;

(10) conducting security inspections and spot checks;

(11) assisting and advising the component regarding the access, dissemination, reproduction, transmission, transportation, safeguarding, and destruction of classified information;

(12) ensuring that proposed public releases on classified programs are reviewed to preclude the release of classified information; and

(13) coordinating and resolving classification and declassification problems.

6. Contracting Officers and Contracting Officer's Technical Representatives shall:

(a) ensure that any contracts that involve classified information meet requirements of the Department of Defense Manual DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM); and

(b) incorporate appropriate security requirements clauses in a classified contract, Invitation for Bid (IFB), Request for Proposal (RFP), Request for Quotation (RFQ), or other solicitation, and provide contractors with the security classification guidance needed during the performance of the contract. This guidance shall be provided to contractors through a Contract Security Classification Specification (DD Form 254). The Contract Security Classification Specification shall identify the specific elements of classified information involved in the contract that require security protection.

7. Individuals Who Have Access to Classified Information shall:

(a) protect it from individuals who do not have authorized access to that information, to include securing it in approved equipment or facilities whenever it is not under the direct control of an authorized individual,

(b) meet safeguarding requirements prescribed by this Order and the Director of Security, M-40, and

(c) take initial and annual training as required, including special training if the individual derivatively classifies information.

8. All Employees and Contractors shall:

(a) learn to recognize classification markings and report any instances where they believe classified information is not properly managed, and

(b) report suspicious activities or behavior that would put classified information at risk of exposure.

IX. IMPLEMENTATION: The policies, procedures, and responsibilities set forth in this Order and its companion manual, DOT Manual 1640.4E, Guide for Managing Classified Information, and the appendices to the manual are for uniform application throughout DOT. Any implementing directives created by Secretarial Offices, Heads of Operating Administrations, Bureaus, and Centers shall meet, and may exceed, the requirements of this Order, manual, and appendices.

DEPUTY ASSISTANT SECRETARY FOR
ADMINISTRATION:

JAN 2 1 2011

Brodi Fontenot