ORDER

1600.2D

SAFEGUARDING CONTROLS AND PROCEDURES FOR CLASSIFIED NATIONAL SECURITY INFORMATION AND SENSITIVE UNCLASSIFIED INFORMATION

August 29, 1997

DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION

istribution: A-WXYZE-3; A-FOF-O (LTD)

Initiated By: ACP-300

FOREWORD

This order provides direction and assigns responsibility for FAA compliance with Executive Order 12958, Classified National Security Information, dated April 20, 1995. The material contained in this order provides direction and guidance regarding the classified information security program as outlined by Executive Order 12958.

Jane F. Garvey
Administrator

TABLE OF CONTENTS

CHAPTER 1. GENERAL

	Page
1. Purpose	1
2. Distribution	1
3. Cancellation	1
4. Background	1
5. Explanation of Changes	2
6. Definitions	2
7. Forms	2
8. Requests for Information	3
9. Authority to Change this Order	3
10. Policy	3
11. Scope	3
12. Responsibilities	4
13. Sensitive Compartmented Information (SCI)	6
14. Supplements to this Directive	6
15.-199. Reserved	6

CHAPTER 2. AUTHORITY TO CLASSIFY INFORMATION

200. General	15
201. Original Classification	15
202. Requests for Classification Authority Pursuant to E.O. 12958	15
203. Original Classification Authority Within the FAA	16
204. Identification and Marking for Originally Classified Material	17
205. Duration of Original Classification	17
206. Classification Guide	18
207. Approval Requirements for Classification Guides	19
208. Coordination Requirements for Original and Revised Classification Guides	19
209. Distribution of Classification Guides	19
210. Derivative Classification	19
211. Responsibility for Assigning Derivative National Security Classification	19
212. Procedures for Applying Derivative Classifications	20
213.-299. Reserved	20

CHAPTER 3. FAA CLASSIFIED NATIONAL SECURITY INFORMATION PROGRAM

300. Purpose 23

SECTION 1. PROGRAM MANAGEMENT 23

301. General 23
302. National Security Information Program Manager 23
303. Designation of the Regional and Center National Security Information Program Managers (RNSIPM & CNSIPM) 25
304. Duties of the RNSIPM and CNSIPM 25
305.-320. Reserved 26

SECTION 2. CLASSIFIED INFORMATION ACCOUNT CUSTODIAN (CIAC) AND ALTERNATE CIAC (ACIAC) 26

321. Designation of the CIAC and the ACIAC 26
322. Duties of the CIAC and the ACIAC 27
323. Designation of Duties of the CIAC and the ACIAC as Performance Outcomes and Expectations 27
324.-329. Reserved 27

SECTION 3. TOP SECRET CONTROL OFFICER (TSCO) AND ALTERNATE TSCO (ATSCO) 27

330. Designation of the TSCO 27
331. Duties of the TSCO 28
332.-335. Reserved 28

SECTION 4. INVENTORIES AND INSPECTIONS 28

336. Classified National Security Information Account Inventories 28
337. Inventory Certification to the SSE 28
338. Reporting Security Violations and Discrepancies 28
339. Procedures for the Conduct of Inventories of TOP SECRET and SECRET Documents 29
340. Inspections 29
341. Inspection Procedures for Classified Information Accounts 30
342.-399. Reserved 30

CHAPTER 4. CLASSIFICATION OF NATIONAL SECURITY INFORMATION

SECTION 1. RULES GOVERNING CLASSIFICATION OF INFORMATION 41

400. Principle 41

401. Classification Levels 41
402. Only Information May Be Classified 41
403. Material Produced by the FAA Containing Classified National Security Information 41
404. Accountability of Classifiers and Classification Documentation 42
405. Classification Approval 42
406. Classification Planning 42
407.-414. Reserved 42

SECTION 2. CLASSIFICATION PRINCIPLES, CRITERIA, AND CONSIDERATIONS 43

415. Original Classification Decisions 43
416. Specific Criteria for Original Classification 43
417. Prohibition of the Use of Other Terms 43
418. Classification Categories 43
419. Presumption of Damage 44
420. Limitations on Classifying Information 44
421. Assigning a Classification to Material Other than Documents 45
422. Assigning a Classification to Information and Intelligence Data Concerning State-of-the-Art Technology 46
423. Effect of Open Publication 46
424. Reevaluation of National Security Classification Due to Compromise 46
425. Assigning a Classification to Compilations 46
426. Classification Review 46
427.-434. Reserved 47

SECTION 3. DURATION OF ORIGINAL SECURITY CLASSIFICATION 47

435. General 47
436. Challenges to National Security Classification 48
437.-443. Reserved 49

SECTION 4. INDUSTRIAL SECURITY OPERATIONS 49

444. Classification in Industrial Security Operations 49
445. Classification Authority 50
446. Independent Research and Development 50
447. Other Private Information 50
448.-499. Reserved 50

CHAPTER 5. DECLASSIFICATION, DOWNGRADING, AND REGRADING

SECTION 1. GENERAL 53

500. Principle 53
501. Authority to Downgrade or Declassify 53
502. Marking Material for Declassification or Downgrading 53
503. Notification to Holders 54
504. Mandatory Review for Declassification 54
505. Processing Requests for Mandatory Review for Declassification 54
506. Classification Review for FOIA Requests 56
507. Remarking Material 56
508.-513. Reserved 56

SECTION 2. DECLASSIFICATION OF TRANSFERRED DOCUMENTS OR MATERIALS 57

514. Material Officially Transferred with a Transfer of Function 57
515. Material Officially Transferred for Storage or Retirement 57
516.-520. Reserved 57

SECTION 3. REGRADING CLASSIFIED INFORMATION 57

521. Regrading to a Higher Classification 57
522. Assigning a National Security Classification to Information Previously Determined to be Unclassified 58
523.-599. Reserved 58

CHAPTER 6. MARKING AND PROCESSING CLASSIFIED INFORMATION

600. Purpose 61
601. Original Classification 61
602. Derivative Classification 61

SECTION 1. THE MARKING PROCESS 61

603. Required Markings 61
604. Portion Marking 62
605. Overall Classification Marking 62
606. The "Classified By" Line 63
607. Recordkeeping Requirements for Classification Based on Multiple Sources 63
608. The "Declassify On" Line 64
609. Downgrading Instructions 64
610. Subject and Title Marking 64
611. Marking Letters of Transmittal 64

SECTION 2. MARKING AND LABELING CLASSIFIED DOCUMENTS AND MATERIALS 65

612. Cover Sheet Requirements for Classified Documents 65
613. Marking Electrically Transmitted Messages 65
614. Marking a National Security Classification on Charts, Maps, and Drawings 66
615. Marking Files with a National Security Classification 66
616. Marking Translations of National Security Classified Information 67
617. Marking Classification on Photographs 67
618. Marking Classified Transparencies and Slides 67
619. Marking Classified Motion Picture Films and Video Recordings 68
620. Marking or Labeling Classified Electronic Recordings and Containers 68
621. Marking or Labeling Classified Electrical Machine and Automated Information System (AIS) Tapes 68
622. Marking Classified AIS Listings 68
623. Marking Decks of Classified AIS Cards 69
624. Remarking of Documents and Other Materials that have been Previously Assigned a Classification 69
625. Marking Unclassified Documents and Materials 70
626. Standard Classification Labels for Media other than Documents 70
627.-630. Reserved. 70

SECTION 3. SPECIAL MARKINGS 70

631. General 70
632. Atomic Energy Information 71
633. Foreign Government Information (FGI) 71
634. Foreign Government "Restricted" Information 72
635. North Atlantic Treaty Organization (NATO) Information 72
636. Intelligence Information 72
637.-641. Reserved. 73

SECTION 4. FOR OFFICIAL USE ONLY (FOUO) 74

642. For Official Use Only (FOUO) Information 74
643. Identification and Marking 74
644.-699. Reserved. 74

CHAPTER 7. ACCESS, DISSEMINATION, AND CONTROL OF CLASSIFIED NATIONAL SECURITY INFORMATION

SECTION 1. ACCESS TO CLASSIFIED INFORMATION 89

700. Policy 89
701. Security Clearance 89
702. Need to Know Principle 89
703. Responsibility for Determining Need to Know and Clearance 90
704. Continuous Evaluation of Eligibility and Administrative Adjustment or Termination of Security Clearance 90
705. Performance Planning and Critical Outcomes and Expectations 91
706.-710. Reserved 91

SECTION 2. DISSEMINATION OF CLASSIFIED INFORMATION WITHIN THE EXECUTIVE BRANCH 91

711. Classified Information Originated by DOT Activities 91
712. Classified Information Originated by Other Departments or Agencies 91
713.-718. Reserved 91

SECTION 3. DISSEMINATION OF CLASSIFIED INFORMATION OUTSIDE THE EXECUTIVE BRANCH 92

719. General Requirements 92
720. Dissemination of Classified Information to the Congress 92
721. Dissemination of Classified Information to the General Accounting Office (GAO) 92
722. Dissemination of Classified Information to the Government Printing Office (GPO) 93
723. Dissemination of Classified Information to the Judiciary 93
724.-730. Reserved 93

SECTION 4. DISSEMINATION OF CLASSIFIED INFORMATION TO FOREIGN GOVERNMENTS, FOREIGN NATIONALS, AND INTERNATIONAL ORGANIZATIONS 94

731. Release of Classified Information to Foreign Governments 94
732. Responsibilities of the FAA 94
733. Release of Military Classified Information 94
734. Release of Other Categories of National Security Classified Information to Foreign Governments 94
735. Responsibilities of the Foreign Government 94

736. Release of Classified Information to Foreign Nationals, Foreign Governments, and International Organizations 95
737. Foreign National Employees 95
738. Access to Classified Information by Foreign National Consultants or Contractors 96
739. Application for Official Visits by Foreign Nationals to FAA Activities where Access to Classified Information May be Involved 96
740.-745. Reserved 97

SECTION 5. RELEASE OF CLASSIFIED INFORMATION TO HISTORICAL RESEARCHERS 97

746. Scope 97
747. Preparation of Request for Access to Classified Information 98
748. Processing Requests for Access to Classified Information 99
749. Duration of Access Approval 99
750. Restrictions on Access to Classified Information 99
751.-755. Reserved 100

SECTION 6. DISSEMINATION OF CLASSIFIED INFORMATION TO FORMER PRESIDENTIAL APPOINTEES, CONTRACTORS, AND OTHERS 100

756. Dissemination of National Security Classified Information to Former Presidential Appointees 100
757. Dissemination of Classified Information to Contractors 100
758. Dissemination of Classified information to National Defense Executive Reservists (NDER) 100
759. Dissemination of National Security Classified Information to the News Media 101
760. Dissemination of National Security Classified Information to Other Recipients 101
761. Dissemination of Classified Information through Meetings 101
762.-770. Reserved 102

SECTION 7. CONTROL OF NATIONAL SECURITY CLASSIFIED INFORMATION 102

771. Accounting Procedures 102
772. Requirement for Establishment of a Security Control Point (SCP) 102
773. Exceptions for Communications Security (COMSEC), Special Intelligence, Registered Publications Systems, Restricted Data, National Security Council Intelligence Information, and Other Unique Material 102

774. SCP Control of Classified Material that is Hand Carried to or from an Activity 103
775. Functions of the SCP 103
776. Requirement For Maintaining FAA Form 1600.35, Classified Document Register 104
777. Controls for Top Secret Classified Information 104
778. Accountability Information to be Entered on the Classified Document Register in the SCP 105
779. Accountability Records for Confidential Material 106
780. Retention of Accountability Records 106
781. Control of Secret and Confidential Working Papers 106
782. Document Control Station (DCS) 107
783.-799. Reserved 108

CHAPTER 8. STORAGE AND SAFEGUARDING OF CLASSIFIED INFORMATION 113

800. General 113
801. Standards for Storage Equipment 113
802. Top Secret Storage 113
803. Top Secret Supplemental Controls 113
804. Secret and Confidential Material Storage 113
805. Secret Supplemental Controls 113
806. Confidential Storage 114
807. Safeguarding Storage Containers and Combinations 114
808. Approval and Inspection Requirement 114
809.-814. Reserved 115
815. Damage and Repair of Approved Security Containers 115
816. Controlled Areas 116
817. Safeguarding Requirements for Closed Areas 117
818. Closed Area Control During Working Hours 117
819. Closed Area Controls During Nonworking Hours 117
820. Restricted Area Controls 118
821. Storage of Classified Material in Vaults 118
822. Storage of Classified Material in Strongrooms 118
823. Supervision of Keys and Locks 119
824. Approved Alarm System 119
825. Automated Access Control Systems 121
826. Electric, Mechanical, or Electromechanical Devices 122
827. Designation of Security Container Custodian 122
828. Duties of the Security Container Custodian 122
829. Identification of Security Containers 123
830. Use of the Security Container Information SF-700 123

831. Use of the Security Container Check Sheet SF-702 123
832. Change of Combinations 124
833. Safeguarding Combinations to Security Containers 124
834. Standard Supply Combination Requirements 125
835. Administrative Safeguard Requirements for Classified Information 125
836. Safeguarding Classified Material During Emergencies 127
837. Emergency Plans 127
838. Relocation of Classified Storage Containers 127
839. Classified Conferences and Meetings 128
840.-899. Reserved 128

CHAPTER 9. REPRODUCTION OF CLASSIFIED INFORMATION

900. Requirement 135
901. Authorization to Reproduce Classified Information 135
902. Local Authorization 135
903. Originator's Authorization for Reproduction of Top Secret 135
904. Accounting for Reproduced Copies of Classified Information 135
905. Marking Reproduced Classified Information 136
906. Reproduction Equipment and Areas 136
907. Control of Office Copiers 136
908. Prohibitions 137
909. Control of Printing and Photographic Areas and Processes 138
910. Production Control Records 138
911. Production Area Controls 138
912. Pressrooms and Bindery Areas 138
913. Composition Area 139
914. Darkrooms 139
915. Proofreading Areas 139
916. Shipping Entrances 139
917. Special Conditions 139
918. Inspection Requirements 140
919.-999. Reserved 140

CHAPTER 10. PACKAGING CLASSIFIED INFORMATION

1000. General 147
1001. Packaging Requirements for Classified Information 147
1002. Requirements for Preparing Classified Packages 148
1003. Receipt Requirements and Tracer Action 148
1004. Packaging Requirements for Nonmailable Bulk Classified Material 148
1005.-1099. Reserved 149

CHAPTER 11. TRANSMISSION OF CLASSIFIED INFORMATION

1100. Requirement 155
1101. Transmission of Top Secret Information 155
1102. Transmission of Secret Information 155
1103 Transmission of Classified Material Via the Department of State Accompanied Diplomatic Pouch System (DOS/ADPS) 157
1104. Returning Classified Material from Overseas Locations 158
1105. Transmission of Secret and Confidential Material Within an Activity or Office 158
1106. Transmission of Bulk Classified Material 159
1107. Transmission of Classified Information by Secure Telecommunications 159
1108. Transmitting Classified Information in Support of Official Visits 159
1109. Transmission by Courier 160
1110. Return of Classified Information Upon Completion of Official Visit 160
1111. Transmission of Classified Information by FAA Employees 160
1112. Courier Travel Within the Contiguous 48 States and Overseas 161
1113. Transporting Classified Information by Courier Aboard Commercial Passenger Aircraft 161
1114. Screening of Classified Material Being Transported by Courier 161
1115.-1199. Reserved 161

CHAPTER 12. DESTRUCTION AND DISPOSAL OF CLASSIFIED INFORMATION

1200. Requirement 169
1201. Preparing Classified Material for Destruction 169
1202. Classified Waste 169
1203. Destruction Methods 170
1204. Destruction Records 170
1205.-1299. Reserved 170

CHAPTER 13. INTERNATIONAL SECURITY REQUIREMENTS

1300. General 177
1301. Policy 177
1302. Governing Federal Laws 177
1303. Foreign Government Information (FGI) 177
1304. Classification Markings on FGI 178
1305. Marking U.S. Documents that Contain FGI 178
1306. Information Classified by a Foreign Entity 178
1307. Classifying Information Provided by a Foreign Entity with an Obligation to Maintain Confidentiality 178
1308. Duration of Classification for FGI 179

1309. Classification Marking for FGI 179
1310. Use of "Restricted" Marking 179
1311. Safeguarding 179
1312. Disclosure Limitations 180
1313. Transmission 180
1314. Reproduction and Disposition/Destruction 180
1315. Loss, Compromise, or Suspected Compromise 180
1316. Control of North Atlantic Treaty Organization (NATO) Material 180
1317. FAA NATO Control Point 181
1318. Control of Classified Information Received in the United States from International Organizations Other than NATO 181
1319. Control of Classified Information Received Overseas from International Organizations Other than NATO 181
1320.-1399. Reserved 181

CHAPTER 14. VISITOR CONTROL

1400. General 185
1401. Visits by FAA Employees to Other Government Facilities 185
1402. Requirements for Use of DOT F 1600.15 or Consolidated Personnel Management Information System (CPMIS) 185
1403. Visitor Categories and Processing Procedures 185
1404. Identification Requirements for Visitors to FAA Facilities 187
1405. Requirement for Maintenance of a Visitor Log 187
1406. Movement Restrictions and Escort Requirements 187
1407. Badging Requirements for Visitors 188
1408. Restrictions on Photography 188
1409. Restrictions on Use of Electronic Recording Devices 188
1410. Reporting Unusual Visitor Interest 188
1411. Visits by FAA Employees to FAA and Other Government Facilities 188
1412.-1499. Reserved 189

CHAPTER 15. COMPROMISES AND SECURITY VIOLATIONS

1500. General 195
1501. Compromise of Classified Information 195
1502. Reporting Security Violations 195
1503. Administrative Inquiries 195
1504. Investigative Requirements in Incidents Involving Probable Compromise 195
1505. Corrective Actions Required Subsequent to Actual or Possible Loss or Compromise of Classified Information Originated by the FAA 196

CHAPTER 15. COMPROMISES AND SECURITY VIOLATIONS

1506. Administrative and Disciplinary Actions 196
1507. Marking Administrative Inquiries and Reports of Investigation 197
1508. Compromises of Cryptographic Information 197
1509. Compromise of Classified Information Originated by a Foreign Government 197
1510.-1599. Reserved 197

CHAPTER 16. MISCELLANEOUS INFORMATION

1600. Operations Security 207
1601. TEMPEST 207
1602. Secure Telephone Unit (STU-III) 208
1603.-1699. Reserved 208

CHAPTER 17. SECURITY EDUCATION

1700. General 213
1701. Responsibilities for Security Education 213
1702. Program Design 213
1703. Indoctrination Briefing 214
1704. Refresher Briefing 214
1705. Reporting Contacts with Foreign Nationals 214
1706. Processing Reports of Contacts with Foreign Nationals 214
1707. Debriefings 215
1708.-1799. Reserved 215

APPENDIX 1. GLOSSARY OF TERMS (10 PAGES) 1
APPENDIX 2. FORMS (2 PAGES) 1
APPENDIX 3. CLASSIFICATION GUIDE (4 PAGES) 1
APPENDIX 4. MARKING CLASSIFIED INFORMATION (12 PAGES) 1
APPENDIX 5. FOREIGN AND INTERNATIONAL ORGANIZATION SECURITY CLASSIFICATIONS (6 PAGES) 1
APPENDIX 6. EXTRACTS FROM U.S.C. TITLE 18 AND TITLE 50 (8 PAGES) 1

APPENDIX 7. CONSTRUCTION REQUIREMENTS FOR CONTROLLED AREAS (6 PAGES) 1
APPENDIX 8. SAMPLE COURIER LETTER (2 PAGES) 1
APPENDIX 9. CLASSIFIED MATERIAL COURIER INSTRUCTIONS (2 PAGES) 1
APPENDIX 10. REQUIREMENTS FOR SAFEGUARDING SENSITIVE BUT UNCLASSIFIED INFORMATION (7 PAGES) 1

CHAPTER 1. GENERAL

1. PURPOSE. This order implements Executive Order (E.O.) 12958, Classified National Security Information, and applicable Department of actions, downgrading, declassification, and safeguarding of classified national Transportation (DOT) policies and procedures. It establishes Federal Aviation Administration (FAA) policy for the protection of classified national security information and sensitive unclassified information. It establishes procedures for original and derivative classification security information.

2. DISTRIBUTION. This order is distributed to the branch level in Washington headquarters, regions, and centers, to overseas area offices, with a limited distribution to all field offices and facilities.

3. CANCELLATION. Order 1600.2C, National Security Information, dated October 17, 1988, and Order 1600.15D, Control and Protection of "FOR OFFICIAL USE ONLY" Information, dated September 6, 1972, are canceled.

4. BACKGROUND. E.O. 12958, Classified National Security Information, dated April 20, 1995, prescribes a uniform system for classifying, safeguarding, and declassifying national security information. E.O. 12958 is implemented within the executive branch by Information Security Oversight Office (ISOO) Directive No. 1. (32 CFR Part 2001), dated October 13, 1995.

a. Presidential Decision Directive (PDD)-29, Security Policy Coordination, dated September 16, 1994, directs the establishment of the Security Policy Board, which is a national-level entity, to coordinate, formulate, evaluate, and oversee the United States Government's security policy in order to achieve coherence and consistency in security policy and a logical nexus between the sensitivity and value of information, capabilities, and assets and the measures used to protect them.

b. E.O. 12958 specifies information that has not previously been disclosed to the public under proper authority may be classified or reclassified after an agency has received a request under the Freedom of Information Act or the Privacy Act of 1974.

c. The National Industrial Security Program Operating Manual (NISPOM), issued January 1995, established by E.O. 12829, January 6, 1993, implements FAA procurement actions which result in the production of classified national security information or sensitive unclassified information or data which requires a cleared contractor to utilize national security information in the performance of the contract.

d. Sensitive but unclassified (SBU) information meets the criteria for exemption from public disclosure set forth under Sections 552 and 552a of 5 U.S.C., Freedom of Information Act and the Privacy Act. SBU describes information which warrants a degree of protection and administrative control that meets the criteria under the

Computer Security Act of 1987, Public Law 100-235. Provisions of 5 U.S.C. Section 552(b) shall be used as a guide in determining what information may be designated "FOR OFFICIAL USE ONLY."

5. EXPLANATION OF CHANGES.

a. The title of this order has been changed to "Safeguarding Controls and Procedures for Classified National Security Information and Sensitive Unclassified Information" to ensure consistency with the terminology used in E.O. 12958.

b. Responsibilities have been updated to reflect changes in the organizational structure.

c. Policies and procedures regarding classified national security data in automated information systems (AIS) have been revised and updated.

d. Information concerning the original classification authority (OCA) has been updated.

e. Order references have been listed without a suffix to indicate the latest edition of the directive.

f. A new requirement has been established for mandatory review every 5 years of classification guides developed by the FAA.

g. Guidelines and procedures for handling different types of sensitive unclassified information have been revised and updated. Additional information regarding the categories listed below is referenced in Appendix 10, Requirements for Safeguarding Sensitive But Unclassified Information.

(1) For Official Use Only (FOUO);

(2) Freedom of Information Act (FOIA) Exemptions;

(3) Limited Official Use (LOU) information;

(4) Sensitive But Unclassified (SBU); and

(5) 14 CFR Part 191, Withholding Security Information from Disclosure Under the Air Transportation Security Act of 1974.

6. DEFINITIONS. The key terms used in this order are listed in Appendix 1, Glossary, together with an explanation of their meanings.

7. FORMS. Appendix 2, Forms, contains a listing of the security forms referred to in this order.

8. REQUESTS FOR INFORMATION. Questions regarding the interpretation of the provisions of this order or their application should be referred in writing to the appropriate FAA security element or to the Office of Civil Aviation Security (CAS) Policy and Planning, ACP, Attn: ACP-300, with an information copy to the Office of CAS Operations, ACO, Attn: ACO-400.

9. AUTHORITY TO CHANGE THIS ORDER. The Associate Administrator for Civil Aviation Security, ACS-1, is authorized to issue changes to this order which do not affect policy, delegation of authority, or assignment of responsibilities.

10. POLICY. It is the policy of the FAA to make available to the public as much information concerning its activities as possible, consistent with the need to protect the national security of the United States. The FAA shall apply security classification only as provided for in the Atomic Energy Act of 1954, as amended, E.O. 12958 as implemented by ISOO implementing instructions, DOT directives, and security bulletins.

11. SCOPE. This order applies to:

a. All FAA employees, military, civilian, and contractor personnel who handle or otherwise are required to have access to classified national security information and data, regardless of duty station, location, or position. The actions pertaining to cleared contractors who utilize classified national security information in the performance of contracts are addressed in paragraph 444 of this order.

b. FAA personnel collocated on military bases, in embassies, or in contractor facilities. Problems in compliance which result from either conflicting priorities or constraints imposed by the non-FAA authority having security cognizance for the facility, installation, or activity where an FAA employee or organizational element is located shall be referred to the appropriate FAA security office for resolution. If the discrepancy concerns requirements of the non-FAA authority that are more stringent than the requirements of this order, the requirements of the non-FAA authority shall take precedence. If, however, the requirements of the non-FAA authority are less stringent than the requirements of this order, this order shall be followed by all FAA personnel and organizational elements. If the matter cannot be resolved at the FAA security office level, it shall be referred through the FAA security office to the Internal Security Division, ACO-400, for a determination. An information copy shall also be provided to the FAA Security Division, ACP-300.

c. The protection of classified national security information processed, stored, or used in or communicated, displayed, or disseminated by AIS. Additional security policy, responsibilities, and requirements applicable specifically to AIS are contained in the latest editions of Order 1600.54, FAA Automated Information Systems Security Handbook, and Order 1600.66, Telecommunications and Information Systems Security Policy.

12. RESPONSIBILITIES.

a. The Associate Administrator for Civil Aviation Security, ACS-1, has overall responsibility for ensuring that classified national security information for which the FAA is responsible is safeguarded, managed, and controlled agencywide in accordance with requirements of E.O. 12958, ISOO Directive No. 1, and applicable DOT policies, directives, and security bulletins.

b. The Office of CAS Policy and Planning, ACP, is responsible for ensuring that policies and procedures for the safeguarding of classified national security information are developed and maintained current. The focal point within ACP for classified national security information is the FAA Security Division.

c. The FAA Security Division, ACP-300, is the focal point within ACP for the development and coordination of policies and procedures for the safeguarding of classified national security information with responsibilities for:

(1) Reviewing agency classified national security information policies regularly to ensure that they are current and conform to national policies.

(2) Taking appropriate action to update, modify, and revise existing agency safeguarding procedures when it is determined that such action is required to meet national policy standards.

(3) Developing new agency safeguarding policies and procedures for approval by the Administrator when required to meet changes in national policies for safeguarding classified national security information.

d. The Office of CAS Operations, ACO, is responsible for implementing the provisions of this order for the safeguarding of classified national security information and monitoring compliance with the agency's safeguarding policies agencywide. The focal point for implementation of the classified national security information program within ACO is the Internal Security Division.

e. The Internal Security Division, ACO-400, is the focal point within ACO for implementation and monitoring of the FAA policies and procedures for safeguarding classified national security information. The responsibilities of this division include:

(1) Conducting inspections, evaluations, and surveys of FAA classified national security information accounts to ensure compliance with the provisions of this order.

(2) Implementing management plans, programs, and techniques for the efficient and cost-effective control, handling, and safeguarding of classified national security information agencywide.

(3) Ensuring that a thorough investigation is conducted at the national headquarters of any event resulting in a loss or compromise of classified national security information and/or violation of the administrative controls for such information prescribed in this order.

(4) Ensuring that appropriate reports required by ISOO and DOT are submitted in a timely manner.

f. The Training and Career Development Staff, ACS-70, shall coordinate with ACO-400 and provide the necessary resources to support a security education and awareness program to train FAA employees with regard to safeguarding classified national security information.

g. The Office of Information Technology, AIT, is responsible for coordinating with ACS in the implementation of the requirements of this order as they apply to classified national security information associated with information resource management (IRM).

h. Assistant Administrators, Associate Administrators, Heads of Offices and Services, Regional Administrators, Director, Mike Monroney Aeronautical Center, and Director, FAA Technical Center, are responsible for ensuring that the provisions of this order are implemented by all elements under their jurisdiction that store, process, transmit, or otherwise are required to have access to classified information or data.

i. Managers of Civil Aviation Security (CAS) Divisions and Staffs are responsible for:

(1) Ensuring that their offices, as servicing security elements (SSE), implement the provisions of this order.

(2) Ensuring that the FAA classified national security information program is implemented within their respective areas of jurisdiction.

(3) Ensuring that all employees within their areas of responsibility who require access to classified national security information or data in any form are properly cleared and are provided with security briefings and indoctrinations in accordance with the requirements of this order.

j. Each FAA Employee Whose Duties Require Him or Her to Have Access to Classified National Security Information is responsible for:

(1) Being familiar with the contents of this order.

(2) Safeguarding, managing, and controlling classified national security information in accordance with the provisions of this order.

(3) Reporting known or suspected violations of the requirements of this order immediately to their supervisor or to the CAS Division or office that is the SSE for their office, facility, or activity or to ACO-400 as the SSE for Washington headquarters.

k. FAA Contractor Personnel are responsible for compliance with the provisions of this order and applicable provisions of the National Industrial Security Program Operating Manual, DOD 5220.22-M, or successor document. Any conflict between these documents shall be reported immediately to ACO-400. ACO-400 shall upon receipt of such a report notify ACP-300, without delay.

13. SENSITIVE COMPARTMENTED INFORMATION (SCI). This term includes all information and materials bearing special community controls indicating restricted handling within present and future community intelligence collection programs and their end products for which community systems of compartmentation have been or will be formally established. The term does not include RESTRICTED DATA as defined in Section 22, Public Law 83-703, Atomic Energy Act of 1954. The Central Intelligence Agency is the cognizant security authority for the FAA receipt, processing, and storage of SCI. The Office of CAS Intelligence, ACI, validates and approves all SCI access requests for the FAA.

14. SUPPLEMENTS TO THIS DIRECTIVE. This order may be supplemented by region and center SSE's as necessary to provide additional instructions pertaining to implementation of the directive within their respective areas of concern.
The appendix method of supplementation is recommended because it provides the user with a cohesive body of organizational procedures and instructions. Regional supplements shall be submitted to ACO-400 for review and approval prior to implementation. An information copy of regional supplements shall be provided to ACP-300 through ACO-400.

15.-199. RESERVED.

CHAPTER 2. AUTHORITY TO CLASSIFY INFORMATION

200. GENERAL. Information which requires protection against unauthorized disclosure in the interest of national security is classified under the authority of E.O. 12958 by an original classification authority (OCA), and is designated and marked as TOP SECRET, SECRET, or CONFIDENTIAL. The designation UNCLASSIFIED is also used to identify information in classified documents and materials which does not require a security classification. Except as otherwise provided by statute, no other terms shall be used to identify classified information. An original classification determination at any level can be made only by a Government official who has been delegated this authority in writing. The OCA may determine that a classification guide is required to identify elements of information being developed and classified for the first time in a particular project. This classification guide will describe the elements of information that require protection, the level of protection, and duration of classification. If a classification guide is issued by the OCA, it shall be cited as the authority for derivative classification decisions involving this information.

201. ORIGINAL CLASSIFICATION. A determination to classify information originally may be made only when: (1) the information falls into one or more of the categories set forth in E.O. 12958 and (2) the unauthorized disclosure of the information, either by itself or in context with other information, reasonably could be expected to cause damage to the national security. The fact that information does fall into one or more of the categories does not mean that it automatically meets the damage criterion, except that unauthorized disclosure of foreign government information, the identity of a confidential foreign source, or intelligence sources or methods is presumed to cause damage to the national security.

202. REQUESTS FOR CLASSIFICATION AUTHORITY PURSUANT TO E.O. 12958.

a. A request for OCA shall be made only when there is a demonstrable and continuing need to exercise such authority and the following conditions exist:

(1) The normal course of operations or missions of the organization results in the origination of information warranting classification;

(2) There is a substantial degree of local autonomy in operations or missions as distinguished from dependence upon a higher level of authority or supervision for relatively detailed guidance;

(3) There is adequate knowledge by the originating level to make sound classification determinations as distinguished from having to seek knowledge from a higher level of authority or supervision; and

(4) There is a valid reason why already designated classification authorities in the originator's chain of authority or supervision have not issued or cannot issue classification guidance to meet the originator's normal needs.

b. Each request for a delegation of OCA shall:

(1) Identify the title of the position held by the nominee and the nominee's organization.

(2) Contain a description of the circumstances consistent with paragraph 202a that justifies the delegation of such authority.

(3) Be submitted through ACS-1 to the Office of Security and Administrative Management, M-70, for forwarding to the Secretary of Transportation.

203. ORIGINAL CLASSIFICATION AUTHORITY WITHIN THE FAA. The Secretary of Transportation is authorized by E.O. 12958 to classify information originally as SECRET and CONFIDENTIAL with further authorization to delegate this authority. This authority has been delegated to the FAA as follows:

a. Normal Conditions. Authority to classify information originally as SECRET and CONFIDENTIAL is delegated to:

(1) The Administrator, AOA-1.

(2) The Associate Administrator for Civil Aviation Security, ACS-1.

b. Authority During Emergency Readiness Levels. The latest edition of Order 1900.1, FAA Emergency Operations Plan, provides guidance concerning conditions under which various FAA readiness levels shall be declared. Authority to classify information originally as SECRET and CONFIDENTIAL is delegated to additional designated FAA officials effective immediately upon declaration of FAA readiness level CHARLIE. If invoked, this authority is automatically terminated when FAA readiness level BRAVO (or a lower level) is declared. Upon declaration of FAA readiness level CHARLIE, the following additional FAA officials are designated as OCA's for SECRET and CONFIDENTIAL:

(1) The Deputy Administrator, ADA-1.

(2) Regional Administrators and the Director, William J. Hughes Technical Center.

(3) The Director, Mike Monroney Aeronautical Center.

c. Delegation of Authority. OCA when delegated is personal and is vested only in the individual occupying the position. The authority may not be exercised "by direction

of" or "for" a designated official. The formal appointment or assignment of an individual to an identified position or a designation in writing to act in the absence of one of these officials, however, has the authority to classify information originally.

d. Training for Officials Designated as OCA's. It is the responsibility of the official authorized to designate an OCA to ensure that all original classification authorities are fully versed in the fundamentals of security classification, limitations of their authority, and their accountability and responsibilities.

204. IDENTIFICATION AND MARKING FOR ORIGINALLY CLASSIFIED MATERIAL. At the time of original classification, each document or other material containing classified information or data shall be marked as specified in Chapter 6, Marking and Processing Classified Information.

a. Application of the required markings indicates that a classification determination has been made.

b. The classification markings identify the persons who receive the material, the level of safeguarding required, and the length of time the information is to be safeguarded at that level.

205. DURATION OF ORIGINAL CLASSIFICATION. The duration of classification for information originally classified shall be determined by specifying a date or event that is 10 years or less from the date of original classification.

a. Information classified under preceding orders that is not subject to automatic declassification and is more than 25 years old shall be marked with a specific date or event for automatic declassification. However, according to E.O. 12958 an agency head may assign an exemption designation to the information only if it qualifies for exemption from automatic declassification and the release of information would reveal:

(1) The identity of a confidential human source, or information about the application of an intelligence source or method, when disclosed to an unauthorized source would clearly and demonstrably damage the national security interests of the United States;

(2) Information that would assist in the development or use of weapons of mass destruction.

(3) Information that would impair U.S. cryptologic systems or activities.

(4) Information that would impair the application of state-of-the-art technology within a U.S. weapon system.

(5) Actual U.S. military war plans that remain in effect.

(6) Information that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States.

(7) Information that would clearly and demonstrably impair the current ability of United States Government officials to protect the President, Vice President, and other officials for whom protection services, in the interest of national security, are authorized.

(8) Information that would seriously and demonstrably impair current national security emergency preparedness plans.

(9) Information that would violate a statute, treaty, or international agreement.

b. Information classified by another agency for which downgrading instructions have not been provided shall remain classified until the originating agency makes a declassification determination.

206. CLASSIFICATION GUIDE. A classification guide is a document issued by an authorized OCA that is the authority for determining the correct level of derivative classification for specified categories of information. The classification guide also indicates the appropriate declassification information. The classification guide must be in a usable format and should be unclassified. Refer to Appendix 3, Classification Guide, for an example of the required format. As a minimum, each classification guide shall meet the following criteria:

a. Identify the Information to be Protected. The classification guide shall use terms necessary to ensure that the information to be protected can be readily and uniformly identified. If the fact that the information exists is assigned a classification as well as the content of the information, this should be clearly pointed out in the classification guide.

b. Specify the Classification Level(s). The classification guide shall state which of the national security classification levels (SECRET or CONFIDENTIAL) applies to the information identified in the guide. The FAA does not have OCA for TOP SECRET.

c. Provide Declassification Guidance. For each element or category of information addressed, the guide shall prescribe declassification instructions such as:

(1) A date on which the element or category of information shall be declassified.

(2) The occurrence of an event after which the element or category of information shall be declassified.

(3) When a document is classified derivatively from source document(s) that contains declassification instruction, "Originating Agency's Determination Required," or OADR, a determination shall be made by an OCA with jurisdiction over the information to re-mark the information to establish a duration of classification consistent with the requirements for information originally classified under this order. See Appendix 4, Marking Classified Information, figure 7.

207. APPROVAL REQUIREMENTS FOR CLASSIFICATION GUIDES. Each classification guide shall be approved personally and in writing by an official who meets at least one of the following qualifications:

a. The individual has program or supervisory responsibility over the information to which the guide pertains.

b. The individual is authorized to classify information originally at the highest level of national security classification authorized in the guide.

208. COORDINATION REQUIREMENTS FOR ORIGINAL AND REVISED CLASSIFICATION GUIDES. Original as well as revised classification guides shall be coordinated with the FAA Security Division, ACP-300, through ACO-400 prior to issue or reissue. Each classification guide shall be reviewed every 5 years by the OCA and updated as necessary.

209. DISTRIBUTION OF CLASSIFICATION GUIDES. The classification guide shall be distributed to offices expected to have a need for it, with copies to ACO-1, ACP-1, and M-70.

210. DERIVATIVE CLASSIFICATION. Derivative classification means the incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. This includes the classification of information based on classification guidance.

211. RESPONSIBILITY FOR ASSIGNING DERIVATIVE NATIONAL SECURITY CLASSIFICATION.

a. Officials who are authorized and required in the performance of their official duties to produce material which is subject to derivative national security classification shall ensure that the information or data are properly classified and that the material is properly marked in accordance with procedures specified in chapter 6.

b. The responsibility for application of derivative national security classification markings includes those persons who are required in the performance of their official duties to incorporate, paraphrase, restate, or generate in new form information that is already assigned a classification; and those persons who are officially responsible for applying classification markings in accordance with a classification guide.

212. PROCEDURES FOR APPLYING DERIVATIVE CLASSIFICATIONS. Specific classification guidance and procedures for applying derivative classification markings are contained in chapter 6 of this order.

213.-299. RESERVED.

CHAPTER 3. FAA CLASSIFIED NATIONAL SECURITY INFORMATION PROGRAM

300. PURPOSE. Order DOT 1640.4C, Classification, Declassification, and Control of National Security Information, requires that the FAA maintain an active national security information management program to ensure compliance with E.O. 12958 and ISOO Directive Number 1. This chapter describes the FAA national security information management structure established in response to these requirements.

SECTION 1. PROGRAM MANAGEMENT

301. GENERAL. ACS has overall responsibility for the FAA classified national security information program. In discharging this responsibility, ACS coordinates with AIT and other FAA offices and services in the development of policies and procedures for safeguarding, controlling, and accounting for classified national security information agencywide.

a. The Office of CAS Policy and Planning, ACP, is the focal point within ACS for researching, developing, and coordinating national security policies and procedures for the implementation of E.O. 12958.

b. The FAA Security Division, ACP-300, is the focal point within the office for classified national security information policy.

c. The Office of CAS Operations, ACO, is responsible for the oversight and operational management of the FAA classified national security information program.

302. NATIONAL SECURITY INFORMATION PROGRAM MANAGER. The Manager, Internal Security Division, ACO-400, is designated as the National Security Information Program Manager (NSIPM). The NSIPM's program management responsibilities include the following:

a. Taking those actions that are necessary to ensure that all FAA employees, contractor employees, and military personnel requiring access to national security classified information or data are familiar with the requirements of this order.

b. Establishing the necessary procedures and resources to oversee, monitor, and conduct evaluations of national, regional, and center compliance with the information security safeguarding, management, control, training, and reporting requirements contained in this order.

c. Monitoring corrective actions taken in regions and at centers with regard to discrepancies and violations involving classified national security and sensitive but unclassified information and data.

d. Ensuring that resources devoted to classified national security information at the national, regional, and center levels are sufficient to support the program requirements identified in this order.

e. Providing information security risk and vulnerability assessments and other specialized guidance and assistance to offices at the national level and to regions and centers when requested.

f. Collecting, analyzing, and maintaining program management statistics as required by this order and the Information Security Oversight Office (ISOO).

g. Coordinating with the Office of Training and Career Development Staff, ACS-70, in the planning, identification, and allocation of the necessary resources at the national level to develop a comprehensive information security education, awareness, and training program to ensure that all FAA employees, military personnel, and contractor employees who require access to classified national security information receive an initial information security indoctrination briefing, an annual update and refresher briefing, and security awareness training on an annual basis or more often if required.

h. Coordinating with ACS-70 and ACP-300 in the development of policies and procedures that support regional and center information security education and training program efforts.

i. Establishing and implementing procedures to ensure the investigation of, and to effectively affix individual responsibility for, incidents of actual or suspected loss, misuse, or negligence with regard to classified national security information or violations of the requirements of this order.

j. For FAA headquarters:

(1) Conducting required inspections of headquarters national security classified information accounts in accordance with requirements of this order.

(2) Taking appropriate followup action to ensure that violations and discrepancies noted as a result of headquarters inspections and surveys are corrected.

(3) Ensuring that semiannual audits of TOP SECRET documents and the annual audits of SECRET documents are accomplished in accordance with the requirements of this order.

(4) Investigating immediately any actual or suspected incident which would indicate possible loss, misuse, or compromise of classified national security information, violation of requirements of this order, or any other action which could

adversely impact the security of classified national security information and data at headquarters.

(5) Identifying any corrective actions necessary because of information developed during an investigation of an incident.

(6) Ensuring that policies and procedures are established to require each classified national security information account to have a Classified Information Account Custodian (CIAC) and at least one Alternate CIAC (ACIAC) designated in writing.

(7) Ensuring that prior to assuming his or her duties, each CIAC and ACIAC satisfies all requirements of this order and the latest edition of Order 1600.1, Personnel Security Program, with regard to security clearance, position sensitivity, and background investigation.

(8) Ensuring that each CIAC and ACIAC is thoroughly familiar with the requirements of this order.

303. DESIGNATION OF THE REGIONAL AND CENTER NATIONAL SECURITY INFORMATION PROGRAM MANAGERS (RNSIPM & CNSIPM). The managers of regional CAS divisions, to include the Europe, Africa, and Middle East Office CAS Division, in their capacity as SSE for the region are also designated as the RNSIPM. The manager of the CAS Staff at the FAA Technical Center and the manager of the CAS Division at the Mike Monroney Aeronautical Center are each designated as the CNSIPM for their respective centers.

304. DUTIES OF THE RNSIPM AND CNSIPM. The RNSIPM and CNSIPM manage their respective regional and center information security programs by performing the regional and center equivalent of each of the duties listed for the NSIPM in paragraph 302 to include the following:

a. Developing and maintaining program management statistics in accordance with guidelines provided by the NSIPM and this order.

b. Conducting required inspections of region and center classified national security information accounts in accordance with requirements of this order.

c. Taking appropriate followup action to ensure that violations and discrepancies noted as a result of the region and center inspections and surveys are corrected.

d. Ensuring that semiannual audits of TOP SECRET documents and the annual audits of SECRET documents are accomplished in accordance with the requirements of this order.

e. Investigating immediately any actual or suspected incident which would indicate possible loss, misuse, or compromise of classified national security information, violation of requirements of this order, or any other action which could adversely impact the security of classified national security information and data within their respective areas of jurisdiction.

f. Recommending any corrective actions necessary because of information developed during an investigation of an incident described in paragraph 302i.

g. Ensuring that for each national security classified information account, a CIAC and at least one ACIAC are designated in writing.

h. Ensuring that prior to assuming his or her duties, each CIAC and ACIAC satisfies all requirements of this order and the latest edition of Order 1600.1, Personnel Security Program, with regard to security clearance, position sensitivity, and background investigation.

i. Ensuring that each CIAC and ACIAC is thoroughly familiar with the requirements of this order.

305.-320. RESERVED.

SECTION 2. CLASSIFIED INFORMATION ACCOUNT CUSTODIAN (CIAC) AND ALTERNATE CIAC (ACIAC)

321. DESIGNATION OF THE CIAC AND THE ACIAC. The manager, supervisor, or higher organizational official of each office, activity, facility, or organizational unit having a classified national security information account shall designate in writing a CIAC and one or more ACIAC's. The official shall document the designation using Form DOT F 1600.31, Document Control Station Establishment Authorization.

a. The individual designated as the CIAC may be the operator of the Security Control Point (SCP) or Document Control Station (DCS).

b. The manager, supervisor, or other official designating the CIAC or ACIAC shall coordinate with the SSE for review of position sensitivity and security clearance status prior to the designated individuals starting their assignments.

c. Before beginning his or her assignment, each CIAC and ACIAC shall have a final security clearance equal to or greater than the highest level of classified information to which he or she would normally require access.

d. The FAA official designating the CIAC or ACIAC is responsible for coordinating with the SSE to arrange for training for the individuals selected before they begin their duties.

322. DUTIES OF THE CIAC AND THE ACIAC. The duties of the CIAC and the ACIAC include but are not limited to the following:

a. Serving as the focal point for the control and safeguarding of classified national security information for their designated areas of responsibility. This includes ensuring that safeguarding, control, and accountability procedures are in compliance with this order.

b. Developing and reporting to the SSE for the region or center the statistical data required to meet ACO-400 and ISOO requirements.

c. Conducting annual audits and inventories of all SECRET documents.

d. Taking immediate action to conduct an inquiry into any known or suspected compromise of classified national security information or violations of security directives, and reporting their findings promptly to their supervisor and to the SSE.

323. DESIGNATION OF DUTIES OF THE CIAC AND THE ACIAC AS PERFORMANCE OUTCOMES AND EXPECTATIONS. The manager, supervisor, or other official responsible for establishing a performance plan for the individuals designated as the CIAC and the ACIAC shall be responsible for the following:

a. Taking appropriate action to establish the duties of the CIAC and the ACIAC as critical outcomes and expectations in the performance plan for each of the individuals designated to fill these positions.

b. Ensuring that the duties performed by the CIAC and the ACIAC are listed in the employee's performance plan.

324.-329. RESERVED.

SECTION 3. TOP SECRET CONTROL OFFICER (TSCO) AND ALTERNATE TSCO (ATSCO)

330. DESIGNATION OF THE TSCO. The TSCO and ATSCO shall be designated in writing by the same authority required to appoint the CIAC. In all cases, individuals designated as TSCO or ATSCO must have a final, current TOP SECRET clearance. The individuals designated as TSCO and ATSCO shall not begin their duties until their designation has been coordinated with, and approved by, the SSE. The TSCO may be

the same individual as the operator of the Security Control Point (SCP). Copies of the TSCO and ATSCO appointment shall be provided to the ACO-400 TSCO through the SSE.

331. DUTIES OF THE TSCO. The TSCO or, in his or her absence, the ATSCO shall receive, safeguard, store, and maintain continuous accountability for and control of all TOP SECRET material received by the office or facility in accordance with the requirements of this order.

332.-335. RESERVED.

SECTION 4. INVENTORIES AND INSPECTIONS

336. CLASSIFIED NATIONAL SECURITY INFORMATION ACCOUNT INVENTORIES. Periodic comprehensive inventories shall be conducted by the SSE of all classified national security information accounts within their jurisdiction. TSCO's, SCP's, DCS's, and CIAC's are subject to both scheduled and unscheduled inventories by the appropriate SSE. In addition, the TSCO and the CIAC shall conduct inventories of their respective accounts in accordance with the requirements of this paragraph.

a. TOP SECRET Material Inventory. A semiannual inventory of all TOP SECRET material within an activity shall be made by the TSCO or the ATSCO in June and December of each year.

b. SECRET Material Inventory. An annual inventory of all SECRET material shall be accomplished by CIAC's in December of each year.

337. INVENTORY CERTIFICATION TO THE SSE. Within 5 work days of the completion of a TOP SECRET or SECRET inventory, written certification of the conduct of the inventory and the results shall be transmitted by the TSCO or the CIAC to the SSE through appropriate region or center channels.

338. REPORTING SECURITY VIOLATIONS AND DISCREPANCIES. If the TSCO or the CIAC becomes aware of any discrepancy in control records, indications of a missing document, or any other discrepancy which would suggest an actual or possible loss or compromise of TOP SECRET, SECRET, or CONFIDENTIAL national security information, the TSCO or the CIAC shall make an immediate verbal report to the SSE by the most expeditious communications means available. The verbal report shall be followed within 24 hours by a detailed written report to the SSE describing in detail the circumstances associated with the loss or discrepancy.

339. PROCEDURES FOR THE CONDUCT OF INVENTORIES OF TOP SECRET AND SECRET DOCUMENTS. The SSE shall, as a minimum, include the procedures listed below in any inventory conducted of TOP SECRET or SECRET national security information.

a. There shall be visual observation of each accountable item of material or evidence of its proper disposition; e.g., the receipt signed by the recipient, destruction certificate, or record of downgrading or declassification.

b. The documents in each container used for the storage of national security classified material must be individually examined to ensure that all TOP SECRET and SECRET material on hand has been entered into the accountability system.

c. Each security storage container used for the storage of TOP SECRET or SECRET information must be examined to ensure that:

(1) The container is a GSA-approved security container that meets the physical security safeguarding standards in chapter 8 of this order and the latest edition of Order 1600.6, Physical Security Management Program, and has been approved in writing by the SSE for safeguarding the level of national security material being stored within.

(2) The container(s) is/are properly managed and controlled.

(3) All of the required forms are attached to the container and are properly filled out as required by this order and the latest edition of Order 1600.6.

(4) The container locking mechanisms are of the proper type and are functioning properly.

(5) The container combination(s) has/have been changed by an authorized person and a copy provided to the SSE in accordance with the requirements of this order and the latest edition of Order 1600.6.

340. INSPECTIONS. A security inspection shall be conducted by the SSE of each classified information account in accordance with the following schedule:

a. Active Accounts. SSE's shall conduct one comprehensive and one supplemental inspection annually for all active accounts.

b. Static Accounts. SSE's shall conduct one comprehensive inspection every 2 years and one supplemental inspection during each intervening year.

c. Followup Inspections. When discrepancies have been noted as a result of an inspection of a classified information account which cannot be corrected on the spot, the SSE shall schedule and conduct a followup inspection to ensure that corrective action has been taken.

341. INSPECTION PROCEDURES FOR CLASSIFIED INFORMATION ACCOUNTS.

a. The SSE shall conduct inspections in accordance with the provisions of this order and the latest edition of Order 1600.6. The inspection shall, as a minimum, include the following:

(1) A thorough examination of the administrative controls and physical safeguards in effect for the safeguarding, control, and accountability of classified information to ensure that they are in compliance with requirements of this order and the latest edition of Order 1600.6.

(2) A random comparison of control records and classified documents to ensure that the control information associated with each document is correct and corresponds with the information on the control log. The SSE should sample from 5 to 10 percent of the total document holdings. For small accounts having 20 documents or less, a 100 percent comparison should be conducted when feasible.

b. The results of the inspection shall be forwarded in the form of a memorandum from the manager of the SSE through established regional or center channels to the appropriate level of management of the office or facility maintaining the classified information account. An information copy of the report shall be provided to the CIAC for the inspected account.

c. When the inspection results in the identification of discrepancies in control procedures, physical safeguards, or any other area affecting the safeguarding of classified national security information, the SSE shall take appropriate action to assist the CIAC in making immediate corrections wherever possible. When discrepancies cannot be corrected immediately, the SSE shall coordinate with the manager or supervisor responsible for the account to ensure that required administrative action is taken to protect classified information until the corrective actions are taken.

d. The SSE shall followup on all discrepancies noted during the course of an inspection of a classified information account to ensure that necessary corrective actions are taken.

e. The SSE shall forward a copy of the inspection report to ACO-400. When a report contains information about violations or discrepancies, the SSE shall also ensure that a copy is forwarded to ACP-300. ACO-400 shall forward copies of reports of violations and discrepancies to M-70 without delay.

342.-399. RESERVED.

CHAPTER 4. CLASSIFICATION OF NATIONAL SECURITY INFORMATION

SECTION 1. RULES GOVERNING CLASSIFICATION OF INFORMATION

400. PRINCIPLE. E.O. 12958 is the only basis for classifying national security information except as provided for in the Atomic Energy Act of 1954, as amended. If there is reasonable doubt about the need to classify information, it shall be safeguarded as classified pending a determination by the Original Classification Authority (OCA). If there is reasonable doubt about the appropriate level of classification, it shall be safeguarded at the higher level of classification pending a determination by the OCA. Followup action shall be initiated by the requesting office if the OCA has not responded within 30 days to a request for a classification determination.

401. CLASSIFICATION LEVELS. Official information which requires protection against unauthorized disclosure in the interest of the national security shall be classified at one of the following three levels:

a. TOP SECRET. The classification TOP SECRET shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the OCA is able to identify or describe.

b. SECRET. The classification SECRET shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the OCA is able to identify or describe.

c. CONFIDENTIAL. The classification CONFIDENTIAL shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause identifiable damage to the national security that the OCA is able to identify or describe.

402. ONLY INFORMATION MAY BE CLASSIFIED. Classified national security information requires protection regardless of its form. It may be expressed orally; in written, photographic, or printed form; or embodied in equipment, on computer disks, magnetic storage media, or any other material. Terms such as classified document, classified material, classified letter, etc., are reference terms to describe items that contain or reveal classified national security information.

403. MATERIAL PRODUCED BY THE FAA CONTAINING CLASSIFIED NATIONAL SECURITY INFORMATION.

a. Only the officials specified in paragraph 203 have authority to make original classification decisions. If another FAA employee generates information believed to warrant original classification, it shall be referred to an OCA for determination.

Pending a classification decision, the material shall be marked with the recommended classification and safeguarded in accordance with this order.

b. Usually, classified information included in material produced by the FAA is based upon classification decisions made outside the agency. The FAA employee producing a document is not originally classifying the information. Rather, the individual is conforming to a classification determination that has been previously reached and is thus making a derivative classification decision.

404. ACCOUNTABILITY OF CLASSIFIERS AND CLASSIFICATION DOCUMENTATION. FAA officials who originally classify information or who make derivative classification determinations shall be held accountable for their decisions and are responsible for maintaining adequate written justification to support those decisions. For an original classification determination, the appropriate justification shall be maintained with the record copy of the document. For a derivative classification, the identification of the source document or classification guide reference upon which the classification is based shall be included with the record copy of the document. If the derivative classification is based on multiple sources, the record file shall contain a list identifying each source. A copy of this list shall be provided to the security control point (SCP) and the document control station (DCS).

405. CLASSIFICATION APPROVAL.

a. When an official approves a document or material marked with a particular level of classification, he or she shall review the information to determine if the classification is appropriate. If there is doubt about the classification level, the document shall be safeguarded at the higher level of classification while a request for classification determination is made to an OCA. Followup action shall be initiated by the requesting office if the OCA has not responded to a request for a classification determination within 30 days.

b. A higher level official who signs or approves a classified document or other classified material is jointly responsible with the accountable classifier for the classification(s) assigned.

406. CLASSIFICATION PLANNING. Advance classification planning is an essential part of the development of any plan, operation, program, research and development project, or procurement action that involves classified information. Classification must be initially considered to ensure protection of the information and the activity.

407.-414. RESERVED.

SECTION 2. CLASSIFICATION PRINCIPLES, CRITERIA, AND CONSIDERATIONS

415. ORIGINAL CLASSIFICATION DECISIONS. Reasoned judgment shall be exercised in making classification decisions. Both advantages and disadvantages of assigning a classification must be weighed. If there is significant doubt about the need to classify information, it shall not be classified. This provision does not amplify or modify the substantive criteria or procedures for classification or create any substantive or procedural rights subject to review. If there is reasonable doubt that the information should be classified, the information shall be safeguarded as if it were classified and a request for classification determination made to an OCA. When a request for a classification determination has been submitted, followup action shall be initiated by the requesting office if the OCA has not responded to the request within 30 days.

416. SPECIFIC CRITERIA FOR ORIGINAL CLASSIFICATION. Before information may be assigned an original classification by an OCA, it must be identified exactly and meet all of the criteria listed below. The fact that the information falls under one or more of the national security classification criteria shall not be presumed to mean that the information automatically qualifies for a classification. All of the following criteria apply:

a. The information must be classified by an OCA who has been properly designated in writing, and who has received training in the duties, responsibilities, and limitations of an OCA.

b. The Government must own, have a proprietary interest in, or otherwise control the information.

c. The information must meet one or more of the categories in paragraph 418.

d. The unauthorized disclosure of the information reasonably could be expected to cause damage to the national security.

417. PROHIBITION OF THE USE OF OTHER TERMS.

a. No other terms shall be used to identify classified national security information except as expressly provided by statute.

b. No other levels, such as sensitive, conference, agency, limited official use, or administrative shall be used in the FAA in conjunction with the national security classification levels as specified in paragraph 401.

418. CLASSIFICATION CATEGORIES. Information shall be considered for classification if it concerns one or more of the following:

a. Military plans, weapons, or operations.

b. The vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security.

c. Foreign government information.

d. Intelligence activities (including special activities) or intelligence methods or sources.

e. Foreign relations or foreign activities of the United States.

f. Scientific, technological, or economic matters relating to national security.

g. U.S. Government programs for safeguarding nuclear materials or facilities.

h. Cryptology.

i. Confidential source(s).

j. Other categories of information which are related to national security and which require protection against unauthorized disclosure as determined by the President or by the Secretary of Transportation with respect to DOT-developed information. Recommendations by FAA personnel concerning the need for any such additional national security classification shall be forwarded through ACS-1 to M-70 for forwarding to the Secretary of Transportation. If and when the Secretary approves a request to classify specific FAA information in these categories, each such determination shall be reported promptly by ACS-1 to M-70 for reporting to the Director of the Information Security Oversight Office (ISOO).

419. PRESUMPTION OF DAMAGE. Unauthorized disclosure of foreign government information, the identity of a confidential foreign source, or intelligence sources and methods are presumed to cause damage to the national security.

420. LIMITATIONS ON CLASSIFYING INFORMATION.

a. Classification may not be used to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; or to restrain competition.

b. Information not clearly related to the national security may not be classified.

c. A product of nongovernment research and development that does not incorporate or reveal national security information to which the producer or developer was given prior access may not be classified until, or unless, the Government acquires

a proprietary interest in the product. This prohibition does not affect the provisions of the Patent Secrecy Act of 1952 (35 U.S.C. 181-188).

d. References to national security documents that do not disclose classified national security information shall not be assigned a classification or used as a basis for assignment of a classification.

e. Classification may not be used to limit dissemination of information that is not classifiable under the provisions of this order, or to prevent or delay the public release of such information.

f. The President or an agency head or official designated under Sections 1.4(a)(1) and (a)(2) of E.O. 12958 and in paragraph 203a (1)(2) of this order may reclassify information previously declassified and disclosed if it is determined in writing that :

(1) Information requires protection in the interest of national security; and

(2) The information may reasonably be recovered. When such reclassification action is proposed within the FAA, the OCA making the proposal shall coordinate the proposed action with the SSE in regions and centers or ACO-400 in the national headquarters. The SSE or ACO-400, as appropriate, shall notify ACS-1 of the proposed action. At the time that the reclassification action is taken, ACS-1 shall inform M-70, who will, in turn, report the reclassification to ISOO.

g. Once the FAA has received a request for information under the Freedom of Information Act (5 U.S.C. 552, as amended, hereinafter referred to as FOIA) or the Privacy Act (5 U.S.C. 552a) or the mandatory review provisions of E.O. 12958, only the Office of the Secretary may classify it or reclassify it.

h. Every effort should be made to classify a document properly at the time of origin. However, when an office believes that a document subject to one of these requests may warrant classification or reclassification, it shall contact its SSE. The SSE shall transmit the request through ACO-400 to M-70.

421. <u>ASSIGNING A CLASSIFICATION TO MATERIAL OTHER THAN DOCUMENTS</u>.

a. Equipment or other physical objects may be assigned a classification only when classified information would be derived by visual observation of their internal or external appearance or structure; or by observing an operation, test, or other application or use of such equipment or objects. The overall classification assigned to such equipment or objects shall be at least as high as the highest classification of any of their integrated parts.

b. If unauthorized knowledge of the existence of an item would cause adverse impact on, compromise, or damage the national security, information concerning the existence of the item could warrant classification.

422. ASSIGNING A CLASSIFICATION TO INFORMATION AND INTELLIGENCE DATA CONCERNING STATE-OF-THE-ART TECHNOLOGY. Assignment of a classification requires consideration of information available from intelligence sources concerning the extent to which the same or similar technology is known or is available to others. It is also important to consider whether it is known publicly or internationally that the United States has the technology or is even interested in the subject matter. The state of technology in other nations is often a vital consideration when considering assignment of a national security classification.

423. EFFECT OF OPEN PUBLICATION. The fact that information currently assigned a national security classification has been disseminated by a public medium of communication does not automatically mean that the information has been declassified. The classification shall continue until the originating agency or higher authority advises to the contrary. Questions regarding the propriety of continuing the classification shall be brought promptly to the attention of the originator. If the originator cannot be readily identified, questions concerning the classification shall be forwarded through ACS-1 to M-70.

424. REEVALUATION OF NATIONAL SECURITY CLASSIFICATION DUE TO COMPROMISE. Classified national security information that may have been subjected to compromise shall be evaluated to determine if it should remain classified. Upon learning of a possible compromise of classified national security information, FAA employees shall report this information by the most expeditious means through their supervisory channels to the SSE.

425. ASSIGNING A CLASSIFICATION TO COMPILATIONS. Normally, a classification will not be assigned to compilations of unclassified items of information. However, certain information that would otherwise be unclassified may require a classification when combined or associated with other unclassified information. In these circumstances, classification may be required if the combination of unclassified items of information provides an added factor that warrants assignment of a classification. Assignment of a classification shall be fully supported by a written explanation provided with the material to be classified.

426. CLASSIFICATION REVIEW.

a. All national security material produced by the FAA is subject to a classification review by the SSE. The manager of the SSE shall ensure that a routine process is established and implemented for the classification review of national security

materials. The classification review shall ensure, among other requirements, that the document(s) is (are) appropriately marked in accordance with the requirements contained in this order in chapter 6.

b. All national security documents produced within the FAA shall be reviewed by SSE personnel prior to transmission from the headquarters or regional office, or when such material produced by a subordinate FAA element is received into the facility. If SSE personnel are not available, the review shall be conducted by the CIAC. In conducting the review, the SSE or the CIAC shall use reasonable care and good judgment in inspecting the documents to ensure that the documents are properly marked and that they have been transmitted and safeguarded in accordance with the provisions of this order.

c. An exception to the pre-transmittal security review is authorized for field activities which produce only a minimal number of national security documents and do not have SSE personnel available, provided that each annual security inspection of the activity by the SSE shall include appropriate review of all national security documents produced since the last inspection.

427.-434. RESERVED.

SECTION 3. DURATION OF ORIGINAL SECURITY CLASSIFICATION

435. GENERAL. The duration of classification for information is determined by an OCA who will follow the sequence listed below:

a. If the information has been assigned an original classification, the OCA shall attempt to determine a date or event that is less than 10 years from the date of original classification and which coincides with the lapse of the information's national security sensitivity, and shall assign such date or event as the declassification instruction.

b. If unable to determine a date or event of less than 10 years, the OCA shall assign a declassification date that is 10 years from the date of the original classification decision.

c. The OCA may assign an exemption designation to the information only if the information qualifies for exemption from automatic declassification.

d. Information assigned a classification under preceding orders that is not subject to automatic declassification shall retain its classification until reviewed for declassification.

e. Information assigned a classification by another agency shall retain its assigned classification until the originating agency makes a declassification determination.

f. If the OCA cannot determine an earlier specific date for declassification, the information shall be marked for declassification 10 years from the date of the original decision except if it applies to:

(1) revealing an intelligence source, method, or activity, or a cryptologic system or activity;

(2) revealing information that would assist in the development or use of weapons of mass destruction;

(3) revealing information that would impair the development or use of technology within a U.S. weapons system;

(4) revealing U.S. military plans or national security emergency preparedness plans;

(5) revealing foreign government information;

(6) damaging relations between the United States and a foreign government, reveal a confidential source, or seriously undermine diplomatic activities that are reasonably expected to be ongoing for a period greater than 10 years;

(7) impairing the ability of responsible U.S. Government officials to protect the President, the vice president, and other individuals for who protection services, in the interest of national security, are authorized; or

(8) violating a statue, treaty, or international agreement.

436. CHALLENGES TO NATIONAL SECURITY CLASSIFICATION. If holders of classified information produced by, or under the cognizance of, the FAA believe that the information has been assigned a classification improperly or unnecessarily, or that an overly restricted period for the duration of the classification has been assigned, they are encouraged to discuss this with a representative of the SSE. The SSE shall seek resolution of such challenges through coordination with the OCA. When requested, the SSE shall maintain the anonymity of the challenger.

a. Challenges made under the provisions of this paragraph and paragraph 504, Mandatory Review for Declassification, must include a description of the information or document being challenged that is sufficient to permit identification with reasonable effort, and must include the reason for the challenge.

b. Challenges to a national security classification must be acted on within 30 days. The challenger shall be notified of the action taken or the fact that no change was

made. Within the FAA, the SSE shall advise the challenger, after coordination with ACO-400, that the decision may be appealed to ACS-1 within 30 days.

c. Within 30 days after receipt of an appeal, ACS-1 may reverse, amend, or uphold the initial decision of the FAA classifier. Through the SSE, ACS-1 shall inform both the challenger and the classifier of the decision and of the option of further appeal to M-70.

d. The information in question shall be safeguarded as required for the classification level initially assigned pending final determination of the challenge to the classification and the results of any appeal.

e. The fact that an FAA employee has challenged a national security classification assignment shall not in any way result in, or serve as the basis for, an adverse personnel action.

f. The provisions of this paragraph do not apply to or affect declassification review actions under the mandatory review requirements of this order contained in Chapter 5, Declassification, Downgrading, and Regrading.

437.-443. RESERVED.

SECTION 4. INDUSTRIAL SECURITY OPERATIONS

444. CLASSIFICATION IN INDUSTRIAL SECURITY OPERATIONS. On January 6, 1993, the President signed E.O. 12829, which established the National Industrial Security Program (NISP) and amended certain portions of E.O. 10865, Safeguarding Classified Information Within Industry. Section 201 of E.O. 12829 states in part as follows:

a. The Secretary of Defense, in consultation with all affected agencies and with the concurrence of the Secretary of Energy, the Nuclear Regulatory Commission, and the Director of Central Intelligence, shall issue and maintain a National Industrial Security Program Operating Manual. The Secretary of Energy and the Nuclear Regulatory Commission shall prescribe and issue that portion of the Manual that pertains to information classified under the Atomic Energy Act of 1954, as amended. The Director of Central Intelligence shall prescribe and issue that portion of the Manual that pertains to intelligence sources and methods, including sensitive compartmented information.

b. The Manual shall prescribe specific requirements, restrictions, and other safeguards that are necessary to preclude unauthorized disclosure and control authorized disclosure of classified information to contractors, licensee, or grantees.

c. The Manual shall apply to the release of classified information during all phases of the contracting process including bidding, negotiation, award, performance, and

termination of contracts, the licensing process, or the grant process, with or under the control of departments or agencies.

445. CLASSIFICATION AUTHORITY. Assignment of a classification to information in U.S. industrial facilities is based on security classification guidance furnished by the Government under the provisions of the NISP, as established by E.O. 12829. Except as amended by Section 203(g) of E.O. 12829, provisions of E.O. 10865 dated February 20, 1960, as amended by E.O. 10909 dated January 17, 1961, and E.O. 11382 dated November 27, 1967, remain in force. Industrial management does not make original classification decisions but applies the national security classification decisions of the contracting authority to information and material developed, produced by, or handled by the Government contracting facility.

446. INDEPENDENT RESEARCH AND DEVELOPMENT.

a. Information that is a product of Government-sponsored independent research and development conducted without access to classified information may not be assigned a classification unless the Government first acquires a proprietary interest in the product.

b. If no prior access was given, but the person or company conducting the independent research or development believes that protection may be warranted in the interest of national security, the information shall be safeguarded as if it were assigned a classification. Where the FAA is the organization of primary concern, the information should be submitted to ACS-1 for evaluation. ACS-1 shall determine if a classification would be assigned if the information belonged to the Government. If the determination is negative, the originator of the information shall be advised that the information is unclassified. If the determination is affirmative, the FAA shall determine whether a proprietary interest in the research and development will be acquired. If such an interest is acquired, the information shall be assigned the proper classification. If proprietary interest is not acquired by the Government, the originator shall be informed that there is no basis for assigning a classification and the tentative classification assigned shall be canceled.

447. OTHER PRIVATE INFORMATION. The procedures specified above shall also apply in cases such as an unsolicited contract bid in which private information is submitted to an FAA element for a determination of national security classification.

448.-499. RESERVED.

CHAPTER 5. DECLASSIFICATION, DOWNGRADING, AND REGRADING

SECTION 1. GENERAL

500. PRINCIPLE. Information that has been assigned a proper national security classification when developed does not necessarily require protection indefinitely. Most classified information has a diminishing significance to the national security as time passes and as technological or other developments occur. When the national security no longer requires that specific information remain classified, it shall be declassified. When the national security requirements are such that the information can be adequately protected at a lower level of classification, it shall be downgraded. Under circumstances where information is judged to require additional protection, regrading provides a means for increasing the classification level provided the appropriate conditions established by E.O. 12958 are met.

501. AUTHORITY TO DOWNGRADE OR DECLASSIFY.

a. Originally Classified Material. Original classification authorities (OCA), a successor, or a supervisory official of either; a higher authority than the original classifier; and the DOT Departmental Security Review Committee are authorized to downgrade or declassify information originally assigned a national security classification by the FAA.

b. Derivatively Classified Material. The declassification authorities designated above and FAA regional and center SSE's are authorized to declassify or downgrade material that has been assigned a derivative classification in accordance with instructions from the applicable classification guide, source document, or OCA. Classification guides and source documents shall, wherever possible, indicate specific dates or events upon which the downgrade or declassification action shall take place. An OCA may downgrade or declassify information in accordance with provisions of E.O. 12958 and this order.

502. MARKING MATERIAL FOR DECLASSIFICATION OR DOWNGRADING.

a. Material which derives its classification from information assigned a classification on or after August 1, 1982, shall be marked with the same declassification instructions found on the source document(s).

b. Material that derives its classification from information assigned a classification prior to August 1, 1982, shall be treated as follows:

(1) If the source material indicates a declassification date or event 20 years or less from the date of origin, that date or event shall be carried forward on the new material.

(2) If the source material bears a downgrading date or event, that date or event shall be carried forward on the new material.

503. NOTIFICATION TO HOLDERS.

a. The appropriate authority responsible for declassification action shall notify all known holders when information is declassified unless the declassification is predetermined to occur automatically.

b. This notification shall include the name and title of the authority for the declassification and the effective date. Notification may be by general notice rather than personal notice provided the general notice will achieve the intended results.

504. MANDATORY REVIEW FOR DECLASSIFICATION.

a. E.O. 12958 requires that procedures be established to handle requests by a U.S. citizen, permanent resident alien, Federal agency, or State or local government to declassify and release information which is considered to have too high a classification or to have been improperly classified in the first place. A request must sufficiently describe the information to permit the record to be identified and located. The time required for responses to mandatory declassification review requests is governed by the amount of search and review time required to process them. After review, the record or any reasonably segregable portion that no longer is of national security concern shall be declassified and released unless withholding is otherwise warranted under applicable laws.

b. Requests for classified records under the Freedom of Information Act (FOIA), as amended, are processed separately from requests made under mandatory review provisions.

c. In response to a request to an agency for a classified document under the FOIA or a mandatory classification review, the agency holding the document may not refuse to confirm the existence or nonexistence of the document unless the fact of its existence or nonexistence would itself require classification.

505. PROCESSING REQUESTS FOR MANDATORY REVIEW FOR DECLASSIFICATION.

a. The Department of Transportation, Office of Security, M-70, 400 7th Street, SW, Washington, DC 20590, is designated as the office to which a member of the public or other department or agency identified in E.O. 12958 will submit a request for the mandatory review for declassification of national security classified material held by DOT. FAA elements which receive a request directly shall immediately notify M-70, through ACS-1.

b. If the request involves material produced by or under the cognizance of the FAA, M-70 will forward the request to ACS-1 for action.

c. ACS-1 shall designate an office to handle the request. This office shall:

(1) Acknowledge receipt of the request to the individual or agency concerned and provide a copy of the correspondence to M-70 through ACS-1.

(2) Notify the requester that no further action can be taken without specific identification of the records in question, if a request does not reasonably describe the records sought.

(3) Conduct a security review which shall include consultation with the office which produced the material and with the source authorities. This shall be done only when the classification or exemption of material from automatic declassification is based upon a decision by an OCA.

(4) Ensure that the requester is notified in a timely manner, usually within 30 to 45 days, of any determination made with regard to the request. If a determination has not been made within 45 days, the designated office shall provide the requester with an explanation in writing as to why additional time is necessary and shall provide a copy of the notification or explanation to M-70 through ACS-1.

(5) Advise the requester in writing, if the office determines that the classification is still required, that if he or she wishes to appeal, the requester can do so to the Department of Transportation, Office of the Assistant Secretary for Administration, Chairperson, Security Review Committee, M-1, 400 7th Street, SW, Washington, DC 20590. Include in the notification to the requester a statement concerning the reason why the requested material cannot be declassified. The office shall also notify the requester that he or she may appeal if the requester has not been notified of a decision after 60 days.

(6) Coordinate with the office that produced the material and ensure that it is declassified and remarked accordingly, if the office determines that the assigned classification is not required, the designated office shall then refer the request to the Director of the Office of Public Affairs, OST, or to the head of whichever organization received the request for review, as appropriate, to determine if it is otherwise available for public release.

d. Declassification of material as a result of a declassification review does not preclude offices from withholding it if it is otherwise exempt from disclosure under the FOIA.

506. CLASSIFICATION REVIEW FOR FOIA REQUESTS.

a. If a record requested under the FOIA is classified, the office with primary responsibility for processing the request shall consult with the appropriate SSE to arrange for a classification review.

b. If it is determined as a result of the classification review process that the information in the requested record no longer requires a classification, the record shall be declassified, the FOIA action office shall be advised, and a determination of releasability shall be made without further reference to security considerations. The fact that a record was at one time assigned a classification and is now declassified is not pertinent to a determination of the releasability of the information under the FOIA. A copy of the declassification decision from the classification review shall be sent to ACS-1 who shall forward it to M-70.

c. If the classification review indicates that the information still requires a national security classification, the SSE shall advise the FOIA action office of this fact prior to the expiration of the time limit for response to the request. The FOIA action office shall notify the requester that the request has been denied pursuant to the provisions of 49 CFR Part 7, Subpart C, section 7, Initial Determination.

d. If the classification review cannot be completed within the specified time limit, the SSE shall inform the FOIA action office. The action office shall arrange for an extension of time in accordance with the provisions of the FOIA.

e. If, as a result of the classification review, a determination is made by the SSE that information requested under the FOIA must retain its classification, a copy of the written justification for the determination to deny based on the results of the classification review shall be forwarded without delay to ACS-1. ACS-1 shall in turn expeditiously provide the determination to M-70 for referral to the Departmental Security Review Committee for its classification review of the entire package.

507. REMARKING MATERIAL. Material which no longer requires a classification shall be declassified and marked to show that it has been downgraded to unclassified. Material that continues to require assignment of a classification shall be marked to indicate clearly that a review was conducted and the date of the review. When possible, a date for taking declassification action shall be established at the time of the review and the material and accountability records pertaining to the material so annotated.

508.-513. RESERVED.

SECTION 2. DECLASSIFICATION OF TRANSFERRED DOCUMENTS OR MATERIALS

514. MATERIAL OFFICIALLY TRANSFERRED WITH A TRANSFER OF FUNCTION. Classified material that is officially transferred to DOT with a transfer of function, and not merely for storage, shall be considered originated by DOT for the purpose of downgrading and declassification. Classified material in the custody of the FAA originated by a department or agency which has ceased to exist, and for which there is no successor agency, and whose functions and records were not officially transferred to another department, may be downgraded or declassified by the authorized FAA holders of the material in accordance with this order and with the prior concurrence of the SSE and ACO-400. If another department or agency has an interest in the matter, the SSE shall ensure that the department or agency concerned is advised of the intent to downgrade or declassify. When such notification is given, the department or agency shall be allowed 30 days to express an objection, if desired, before downgrading or declassification action is taken. Differences of opinion which cannot be resolved by the SSE or ACO-400 shall be referred to the DOT Departmental Security Review Committee through ACS-1.

515. MATERIAL OFFICIALLY TRANSFERRED FOR STORAGE OR RETIREMENT. When classified material is being prepared for transfer to a records center or to the National Archives for storage or retirement, the manager of the FAA office or activity responsible for preparing the material shall coordinate with the SSE to ensure that procedures are followed for remarking each document to reflect the current classification. The documents shall be reviewed to determine if they can be downgraded or declassified. If no changes are warranted, the FAA manager or supervisor responsible for preparing the documents for shipment shall certify in writing that a classification review was conducted. This information shall be shown on the document or on the SF-135, Record Transmittal and Receipt Form. If the review results in changes in classification, the responsible manager or supervisor, in coordination with the SSE, shall implement the procedures for notification of changes in classification specified in paragraph 503.

516.-520. RESERVED.

SECTION 3. REGRADING CLASSIFIED INFORMATION

521. REGRADING TO A HIGHER CLASSIFICATION. If it is determined by appropriate authority that the classification assigned to specific information must be upgraded to a higher level in the interests of national security, the authority making the determination shall promptly notify the SSE and all known addressees and holders of the information of the action taken. All affected material shall be promptly remarked to indicate the classification change; the name, title, and address of the individual authorizing the

action; date of the action; and the identity of the person taking the action. The appropriate logs and other accountability records shall also be amended to reflect the change.

522. ASSIGNING A NATIONAL SECURITY CLASSIFICATION TO INFORMATION PREVIOUSLY DETERMINED TO BE UNCLASSIFIED. The President, an agency head, or other official who has been designated in writing as an OCA, may reclassify information previously declassified and disclosed if it is determined both that the information requires protection in the interests of national security and that the information can be reasonably recovered.

523.-599. RESERVED.

CHAPTER 6. MARKING AND PROCESSING CLASSIFIED INFORMATION

600. PURPOSE. Material assigned a classification (including hardware, instrumentation, equipment, etc.) shall be marked to indicate that a classification determination has been made. The purpose of marking classified national security material is to inform holders that it requires protection. Marking also assists in extracting or paraphrasing information from a classified document. Classification marking is simply the physical act of indicating the national security classification level assigned and any special limitations on dissemination. In addition to marking the classification level, declassification markings are required, to include downgrading and any other special handling procedures. All markings must be affixed to the various types of material in a prescribed manner.

601. ORIGINAL CLASSIFICATION. Original classification is a first-time decision that previously unclassified information requires protection against unauthorized disclosure. Only individuals specifically designated in writing as original classification authority (OCA), and who have received appropriate training to be OCA's, may classify documents originally.

602. DERIVATIVE CLASSIFICATION. Derivative classification is a determination that information is the same as that already classified. It is the act of incorporating, restating, or generating in new form information that is already classified, and marking the new material with the same markings as the source information. The source information is also referred to as source documents. The majority of FAA classification involves derivative classification. Only individuals with the appropriate security clearance who have been designated in writing as having derivative classification authority, and who are required by their work to restate classified sources information, may classify derivatively.

SECTION 1. THE MARKING PROCESS

603. REQUIRED MARKINGS. Markings shall be uniformly and conspicuously applied to leave no doubt about the classified status of the information, the level of protection required, and the duration of classification. The following required markings are placed on all classified documents at the time of classification:

a. Portion marking. (See paragraph 604.)

b. Overall classification. (See paragraph 605.)

c. "Classified By" line. (See paragraph 606.)

d. "Declassify On" line. (See paragraph 608.)

e. "Reason" line. The original classifier shall identify the reason(s) for the decision to classify. The classifier shall include, at a minimum, a brief reference to the pertinent classification category (ies) as specified in chapter 4, paragraph 418.

604. PORTION MARKING. The marking process identifies the classification level of each portion of a document. A portion is ordinarily defined as a paragraph or subparagraph. Subjects and titles are also treated as portions. Only in this way can the overall classification level of a document be determined. Refer to Appendix 4, Marking Classified Information, figures 1 through 3.

a. Every part of a classified document, including the subject and/or title, shall have portion classification markings applied. Portion marking eliminates any doubt as to which portions of a document contain classified information. The classification symbol is placed immediately following a subject or title.

b. When marking portions, the following symbols will be used for classification markings:

(1) (TS) - TOP SECRET

(2) (S) - SECRET

(3) (C) - CONFIDENTIAL

(4) (U) - UNCLASSIFIED

605. OVERALL CLASSIFICATION MARKING. After portion marking all parts of the classified document, the next step is to determine the overall classification or highest level of information found in the document. Conspicuously mark the overall classification at the top and bottom of the page in letters larger and bolder than the rest of the text. Refer to appendix 4, figure 4.

a. If the document contains more than one page, place the overall marking at the top and bottom of the outside of the front cover, on the title page, on the first page, and on the outside back cover.

b. If a classified publication is without cover pages, show the overall classification on the first page. Mark other internal pages with the highest classification level of information contained on that page; or, when necessary for production efficiency, mark each internal page with the overall classification of the document. In the latter case, the portion markings will serve as a reliable guide to the classification of each individual page.

606. THE "CLASSIFIED BY" LINE. This step identifies either the Original Classification Authority or the Source of the Classification by name or personal identifier and position. Refer to appendix 4, figures 5 and 6.

a. Originally Classified Information. Identify the classification authority, by office symbol, on the "Classified By" line. If the identity of the originating agency is not apparent on the face of the document, also show the agency. For example:

(1) Classified by: ACS-1
(2) Reason: 1.5(a) and (g)
(3) Declassify on: November 27, 2004

or

(1) Classified by: FAA/ACS-1
(2) Reason: 1.5(a)
(3) Declassify on: December 21, 2004

b. Derivatively Classified Information. If all information in the document is from a single source, identify the source document or classification guide used as the basis for classification. For example:

(1) Derived from: ACS-1 Memo S-000, dated 1/10/93
Subj: Classification Guidance
Reason: 1.5(a) and (g)
Declassify on: October 29, 2004

or

(2) Derived from: CLASS. GUIDE.
(Subj. or ID No. and Date.)
Declassify on: November 30, 2004

NOTE: The "Reason" line, as reflected in the source document(s) or classification guide, is not required to be transferred to the derivative document. If included, however, carry forward the "Reason" as it appears on the source document or as specified in the paragraph 606 b(1).

607. RECORDKEEPING REQUIREMENTS FOR CLASSIFICATION BASED ON MULTIPLE SOURCES. If the classified information is derived from more than one source document, enter the standard notation "Multiple Sources" next to the "Classified By" line. In addition, a listing of each of the multiple sources of classification must be maintained. This may be shown as a notation on record copies of the document, be included in a bibliography or reference section, or be maintained on related correspondence such as a memorandum for the record.

This recordkeeping process is extremely important in cases where classified documents are involved in Freedom of Information Act (FOIA) and Privacy Act requests. Accurate listings of documents from which classified references were extracted are essential in making damage assessments related to compromise of classified information, or in the conduct of investigations of espionage where there is a requirement for the original classifier to evaluate the classification and releasability of the document.

608. THE "DECLASSIFY ON" LINE.

a. Originally Classified Documents. This essential marking indicates the duration of classification. Determine a date or event that is less than 10 years from the date of original classification based upon the duration of the national security sensitivity of the information. This indicates that the information shall be marked for declassification 10 years from the date of the original decision. Refer to appendix 4, figure 7.

b. Derivatively Classified Documents. If all classified information is derived from a single source, carry forward the declassification instruction from the source document. If multiple sources were used, a document derivatively classified on the basis of that document shall cite the source document on its derived from line rather than the term multiple sources. Refer to appendix 4, figure 8.

609. DOWNGRADING INSTRUCTIONS. It is the responsibility of the original classifier, whenever possible, to predetermine at the time information is classified a date or event upon which the decreased sensitivity of the information will permit its downgrading. Refer to appendix 4, figure 9.

610. SUBJECT AND TITLE MARKING. Subjects and titles should be unclassified if possible. A classified subject or title may be used if absolutely necessary. In such cases, an unclassified short title shall be added for reference purposes. Subjects and titles shall be marked with the appropriate symbol: "(TS)," "(S)," "(C)," or "(U)," placed immediately following and to the right of the subject or title. When appropriate, the symbols "(RD)," for Restricted Data, and "(FRD)," for Formerly Restricted Data, shall be added.

611. MARKING LETTERS OF TRANSMITTAL. Conspicuously mark an unclassified transmittal document with the highest classification level of any information transmitted by it. Also mark the transmittal document with an appropriate instruction indicating the classification when separated from the classified enclosures. If the transmittal document itself contains classified information, mark it as required for all other classified information, except: (1) Conspicuously mark the top and bottom of the transmittal document with the highest classification level of any information contained in the transmittal document or its enclosures; and (2) mark the transmittal document

with an appropriate instruction indicating its overall classification level when separated from its enclosures (e.g., "Downgrade to CONFIDENTIAL when separated from SECRET enclosure").

SECTION 2. MARKING AND LABELING CLASSIFIED DOCUMENTS AND MATERIALS

612. COVER SHEET REQUIREMENTS FOR CLASSIFIED DOCUMENTS. Document cover sheets are used to protect national security classified information against unauthorized disclosure. The appropriate standard forms (SF) listed below shall be affixed to the top of the document and shall remain attached until the document is destroyed or placed in a file in a folder that has the appropriate classification markings. Cover sheets may be removed prior to filing the document.

a. SF 703, TOP SECRET Cover Sheet. (NSN: 7540-01-213-7901) shall be used to protect documents assigned a national security classification of TOP SECRET.

b. SF 704, SECRET Cover Sheet. (NSN: 7540-01-7902) shall be used to protect documents assigned a national security classification of SECRET.

c. SF 705, CONFIDENTIAL Cover Sheet. (NSN: 7540-01-213-7903) shall be used to protect documents assigned a national security classification of CONFIDENTIAL.

d. National Security Council (NSC) documents shall be protected using the special cover sheet prepared and disseminated by the NSC.

613. MARKING ELECTRICALLY TRANSMITTED MESSAGES. Messages assigned a classification shall be marked at the top and bottom with the appropriate classification level. When a message is printed by an automated system, the classification markings may be applied by that same system provided the markings are clearly distinguishable from the printed text.

a. The first item of information in the message text shall state the overall classification of the message.

b. The originator of a classified message shall be considered as the accountable classifier. For this reason there is no requirement for a "Classified By" line.

c. The originator is responsible for maintaining adequate records in the form of actual source documents, letters, or memoranda which provide the data necessary to show the source of any derivative classification assigned. This justification data shall be maintained with the record copy of the message to which the derivative classification has been applied for the duration of the classified life of the message.

d. Downgrading and declassification instructions will be included in the last line or paragraph of an electrical message that has been assigned a classification. The following downgrading and declassification markings shall be used:

(1) Downgrading. The downgrading marking is "DNG:" followed by the appropriate national security classification symbol such as "S" for SECRET and the specific date or event for downgrading action. For example, if a message assigned a national security classification level of SECRET is to be downgraded to CONFIDENTIAL on March 2, 1998, this would be indicated as follows: "DNG: /C/ 3-2-98."

(2) Declassification. If a message is to be declassified after a specific date or event, this information shall be marked on the message following the downgrading instructions. If the message cannot be declassified without the approval of the originating office, this too shall be indicated in the document marking. The following markings are to be used:

(a) When the date on which the message is to be declassified is known, the document shall be marked as follows:

"DECL: (Insert day, month, and year for declassification); e.g., "DECL: 10/11/98,"

(b) When the message is to be declassified after a particular event has taken place, the marking shall be as follows:

"DECL: (Description of event); e.g., "DECL: After the Presidential Inauguration"

(c) If the message cannot be declassified without a determination on the part of the originating agency, it shall be marked as follows:

"DECLASSIFY ON: SOURCE MARKED OADR

614. MARKING A NATIONAL SECURITY CLASSIFICATION ON CHARTS, MAPS, AND DRAWINGS. Charts, maps, and drawings shall bear the appropriate security classification marking under the legend, title block, or scale in such a manner as to differentiate between the classification assigned to the document as a whole and the classification assigned to the title or legend. For example, on a map document which has an overall classification of SECRET the title block may be CONFIDENTIAL.

615. MARKING FILES WITH A NATIONAL SECURITY CLASSIFICATION. File folders, binders, envelopes, etc., containing documents that have been assigned a national security classification shall be conspicuously marked with the highest classification level of the document(s) stored or contained therein.

616. MARKING TRANSLATIONS OF NATIONAL SECURITY CLASSIFIED INFORMATION. When U.S. information that has been assigned a classification is translated into a language other than English, the translation shall be marked to show the United States as the country of origin. The appropriate U.S. classification markings shall be applied, and the document shall also be marked with the foreign language equivalent classification. Translations into English of foreign government information (FGI) that has been assigned a classification by the foreign government shall be marked with the name of the country of origin and the foreign and U.S. equivalent classification. Additional references are stated in appendix 4 section 10-1 and 2.

The higher of the two classification levels shall be marked at the top and bottom of each document. If the classification markings are covered when the document(s) is/are rolled or folded, additional classification markings to reflect the highest classification shall be added that are clearly visible when the document(s) is/are rolled or folded.

617. MARKING CLASSIFICATION ON PHOTOGRAPHS. Photographic negatives and positives shall be marked with the appropriate classification markings and kept in envelopes or containers that are conspicuously marked with the appropriate classification.

a. Roll Negatives shall be marked at the beginning and end of each strip with the appropriate classification.

b. Single Negatives shall be individually marked top and bottom with the appropriate classification.

c. Photographic Prints shall be marked individually with the appropriate classification on the top and bottom of the face side of the print, and where practicable, the center of the reverse side.

d. Self-Processing Film or Paper when used to photograph classified material requires special precautions. Care must be taken to ensure that the negative of the last exposure does not remain in the camera. All component parts of the last exposure shall be removed and destroyed as classified waste or the camera itself shall be stored in the manner prescribed for the highest level of classification contained in the negative.

618. MARKING CLASSIFIED TRANSPARENCIES AND SLIDES. The appropriate classification level shall be marked on each transparency or slide. Other applicable markings (e.g., classified by, regrading, and downgrading data) shall when practicable be placed on the border, holder, or frame.

619. MARKING CLASSIFIED MOTION PICTURE FILMS AND VIDEO RECORDINGS.

a. Motion Picture Film. Motion picture film that has been assigned a classification shall be marked with the classification at the beginning and end of each reel. The classification markings shall be fully visible when projected on the screen. Motion picture reels that have been assigned a classification shall be kept in film cans or other suitable containers which have been conspicuously marked or labeled front and back and on each side with the appropriate classification level. If the motion picture film has a sound track, warning of the classification shall, if possible, be audibly reproduced and included in the introduction and at the end of the film.

b. Video Recordings.

(1) Videotape recordings that contain classified information shall include on the recording itself a conspicuous classification marking at both the beginning and the end.

(2) In addition, the videotape case and the carrying and storage containers shall be conspicuously marked or labeled front and back and on each side with the highest level of classification assigned to the information recorded on the videotape. Where appropriate, the classification of the tape shall also be included as an audio warning on the sound track in the audio introduction to the tape and again at the end of the tape.

620. MARKING OR LABELING CLASSIFIED ELECTRONIC RECORDINGS AND CONTAINERS. Recordings, sound or electronic, shall contain at the beginning and end a statement of the assigned classification which will provide adequate assurance that any listener or recipient will know that classified information of a specified level is involved. The recording material and containers shall also be marked or labeled conspicuously with the appropriate classification.

621. MARKING OR LABELING CLASSIFIED ELECTRICAL MACHINE AND AUTOMATED INFORMATION SYSTEM (AIS) TAPES. Although not in frequent use in the FAA, when classified electrical machine and AIS tapes are encountered they shall be provided with external markings or labels and internal notations sufficient to ensure that any recipient of the tapes will know the level of classified information that is involved. The markings or labels will also serve to alert recipients that the classified information contained on the tapes requires protection when reproduced by any medium, such as terminal displays, printouts, etc.

622. MARKING CLASSIFIED AIS LISTINGS. Classification markings on pages of listings produced by AIS equipment may be applied by the equipment itself on the face of the page provided the markings are clearly distinguishable from the printed text. As a minimum, such listings shall be marked with the classification on the top and bottom of the first and last pages and on the top and bottom of any covers.

623. MARKING DECKS OF CLASSIFIED AIS CARDS. Although the FAA seldom, if ever, uses decks of AIS cards in its modern systems, should the need arise to apply a classification to such cards, the markings shall be applied in accordance with this paragraph. Each card in a deck of AIS cards does not have to be marked individually with the classification if the cards remain together in a deck. In this case, an additional card shall be added to identify the contents of the deck, the number of cards in the deck, and the highest level of classification involved. The markings shall be applied in the same manner as required for a single document, i.e., markings showing the highest level of classification contained in the deck shall be applied to the top and bottom of the first and last cards and on the top and bottom of any covers. When a deck of AIS cards is marked in this manner, it shall be stored, transmitted, destroyed, and otherwise safeguarded, accounted for, and controlled in the manner prescribed by this order for classified documents of the same classification level. Cards removed for separate processing or use and not immediately returned to the deck after processing shall be protected as classified information. In these instances, the cards shall be marked individually as prescribed for standard classified documents.

624. RE-MARKING OF DOCUMENTS AND OTHER MATERIALS THAT HAVE BEEN PREVIOUSLY ASSIGNED A CLASSIFICATION. Whenever documents or other materials that have been assigned a classification are downgraded or declassified, or when their classification level is changed, the document(s) or material(s) shall be promptly and conspicuously marked or labeled to reflect the change(s). The marking or labeling applied shall indicate the authority for the re-marking and the date of the action.

a. Re-marking Classified Material. In re-marking material, the former classification markings and other notations affected shall be heavily lined through or otherwise canceled and the new markings applied. If it is not practicable to re-mark each page of the document, the first or title page shall be amended to explain the markings applied.

b. Re-marking of High Volumes of Classified Documents or Materials. When the volume of information or materials is such that prompt re-marking of each item bearing a classification cannot be accomplished without unduly interfering with operations, the classified information account custodian (CIAC) may attach downgrading, declassification, or upgrading notices to the storage unit or container in which the documents or materials are kept in lieu of the re-marking process otherwise required. Each notice shall indicate the change in classification, the authority for the action, the date of the action, the identity of the person taking the action, and the storage units or containers to which the notice applies. When the individual documents or materials are withdrawn from such storage units or containers, they shall be promptly re-marked or relabeled and the old markings shall be canceled.

c. Moving Classified Materials From One Storage Unit to Another. When information or material subject to a posted downgrading, upgrading, or declassification action is withdrawn from one storage unit or container solely for transfer to another storage unit or container, or a storage unit or container containing classified documents or materials is transferred from one place to another, the transfer may be made without re-marking if the notice specifies the requirements of paragraph 624, above, and is attached to or remains with each shipment.

625. MARKING UNCLASSIFIED DOCUMENTS AND MATERIALS. Normally, wholly unclassified material shall not be marked or stamped unless it must be clearly indicated that a decision has been made not to classify it.

626. STANDARD CLASSIFICATION LABELS FOR MEDIA OTHER THAN DOCUMENTS. When size or configuration of hardware, AIS media, or other media or materials make the application of classification markings by machine or manual stamp difficult, classification labels listed in this paragraph shall be attached to the material(s) to show the classification or other restrictions applicable to each item or component clearly. The label shall be affixed to the medium in a manner that will not adversely affect the operation of equipment in which the medium is used.

a. TOP SECRET media shall be protected by SF 706, TOP SECRET Label (NSN: 7540-01-207-5536).

b. SECRET media shall be protected by SF 707, SECRET Label (NSN: 7540-01-207-5537).

c. CONFIDENTIAL media shall be protected by SF 708, CONFIDENTIAL Label (NSN: 7540-01-207-5540).

d. CLASSIFIED media which contain national security information for which the classifier has not determined the specific national security classification level shall be protected by SF 709, CLASSIFIED LABEL (NSN: 7540-01-207-5539).

627.-630. RESERVED.

SECTION 3. SPECIAL MARKINGS

631. GENERAL. There may be information contained in a document that requires markings in addition to the essential markings described in preceding paragraphs. These markings alert the holder to special requirements for safeguarding the information. This section covers the most commonly encountered special markings.

632. ATOMIC ENERGY INFORMATION.

a. Mark the first page or cover page of information containing Restricted Data (RD) as follows:

"RESTRICTED DATA"
"This material Contains Restricted Data as Defined in the Atomic Energy Act of 1954. Unauthorized Disclosure Subject to Administrative and Criminal Sanctions."

b. Mark the first page or cover page of information containing Formerly Restricted Data with the following:

"FORMERLY RESTRICTED DATA"
"Unauthorized disclosure subject to administrative and criminal sanctions. Handle as Restricted Data in Foreign Dissemination. Section 144.b., Atomic Energy Act, 1954."

c. When both "Restricted Data" and "Formerly Restricted Data" appear in a document, only the "Restricted Data" markings are needed for the overall document or page markings. Use the portion marking symbol "(RD)" for Restricted Data and "(FRD)" for Formerly Restricted Data. Show the portion marking symbols following the classification and separated by a hyphen or slash (i.e., (S/RD) or (S-FRD)). Also place the words "Restricted Data" or "Formerly Restricted Data" at the top and bottom of the page in which the information occurs, after the overall classification.

d. Mark the first page or cover page of Critical Nuclear Weapon Design Information (CNWDI) Restricted Data as follows:

"CRITICAL NUCLEAR WEAPON DESIGN INFORMATION -
DOD Directive 5210.2 applies."

Show the portion marking symbol (N) for CNWDI after the classification and in parentheses (i.e., (S/RD (N)). Since CNWDI information is a type of RD, CNWDI markings will always be accompanied by RD markings as well.

633. FOREIGN GOVERNMENT INFORMATION (FGI). When the security classification on a foreign government document is already shown in English, apply no other markings to the document. If the document displays the foreign classification, mark the overall equivalent U.S. classification on the document. FAA documents that contain FGI shall be marked "FOREIGN GOVERNMENT INFORMATION." In addition, portion mark to identify the foreign government origin; for example, "(FRG-C)," which identifies the information as CONFIDENTIAL originating in the Federal Republic of Germany. See Chapter 10, Packaging Classified Information, and appendix 4, figure 10.

634. FOREIGN GOVERNMENT "RESTRICTED" INFORMATION. Some foreign governments use a fourth classification level designated RESTRICTED. Apply no other classification to a foreign government document marked RESTRICTED or the foreign equivalent of the word, but add the following notation to the face of the document: This classified material is to be safeguarded in accordance with provisions of Chapter 8, Storage and Safeguarding of Classified Information. Foreign "Restricted" information contained in a U.S. document requires protection equal to that required for CONFIDENTIAL material. If an otherwise unclassified document contains foreign "Restricted" information, mark the document CONFIDENTIAL and apply portion marks such as "(FRG-R)." See chapter 10 and appendix 4, figure 10-2.

635. NORTH ATLANTIC TREATY ORGANIZATION (NATO) INFORMATION. Classified documents originated by NATO and not already marked with the appropriate classification in English shall be marked with the U.S. equivalent classification. See chapter 10 for additional information on processing and marking NATO documents. Downgrading and declassification markings are not required.

a. NATO information in FAA documents. Mark "THIS DOCUMENT CONTAINS NATO (classification) INFORMATION" on the cover or first page of documents containing classified information extracted from NATO documents. Show only the U.S. classification on the top and bottom of the document. In addition, portion mark to identify as NATO information; for example, "NATO-S" for NATO SECRET.

b. NATO "RESTRICTED" information. When NATO "RESTRICTED" information is included in unclassified documents, place the following statement on the cover or first page:

> "THIS DOCUMENT CONTAINS NATO RESTRICTED INFORMATION AND SHALL BE SAFEGUARDED AS FOR OFFICIAL USE ONLY INFORMATION." Mark each page containing NATO Restricted information, "This page contains NATO RESTRICTED information."

636. INTELLIGENCE INFORMATION.

a. Documents containing classified intelligence information may be caveated with one or more of the following dissemination caveats:

Full Text	Abbreviated Form	Portion Marking Symbol
NOT RELEASEABLE TO FOREIGN NATIONALS	NOFORN	(NF)
WARNING NOTICE - INTELLIGENCE SOURCES OR METHODS INVOLVED	WNINTEL	(WN)

DISSEMINATION AND EXTRACTION OF INFORMATION CONTROLLED BY ORIGINATOR	ORCON	(OC)
CAUTION - PROPRIETARY INFORMATION INVOLVED	PROPIN	(PR)
THIS INFORMATION HAS BEEN AUTHORIZED FOR RELEASE TO:	RELEASABLE TO:	(REL)

b. Show the long form of a caveat once on the first page and cover, if any. There are no mandatory placement requirements for the long form of a caveat. Show the abbreviated form of the caveat at the top or bottom of the page, following the classification, on any page where the information appears. The abbreviated form can also be used in any situation where the long form is not feasible.

NOTE: The following control markings below are obsolete and will not be used in accordance with this order and implementing DOT guidelines and requirements effective April 12, 1995. These control markings will no longer be used on any newly created documents or other materials after their effective dates.

NOT RELEASABLE TO FOREIGN NATIONALS	NOFORN	(NF),
WARNING NOTICE - INTELLIGENCE SOURCES OR METHODS INVOLVED	WNINTEL	(WN),
THIS INFORMATION HAS BEEN AUTHORIZED FOR RELEASE TO,	RELEASABLE TO	(REL), and
NOT RELEASABLE TO CONTRACTORS OR CONTRACTORS CONSULTANTS	NOCONTRACT	(NC).

It is not required to control the material with the caveats as specified above, and holders of material bearing these markings may line through or otherwise remove the marking(s) from documents or other material. INFORMATION MARKED NOFORN BEFORE THE DATE SPECIFIED ABOVE SHALL CONTINUE TO BE MARKED AND NOT BE RELEASED TO FOREIGN NATIONALS.

637.-641. RESERVED.

SECTION 4. FOR OFFICIAL USE ONLY (FOUO)

642. "FOR OFFICIAL USE ONLY" (FOUO) INFORMATION. Unclassified information which is to be protected against uncontrolled release is considered to be FOR OFFICIAL USE ONLY and this term is prescribed for use within FAA to signify such information. FOR OFFICIAL USE ONLY is not a classification term. It denotes unclassified information which requires protection against indiscriminate handling.

643. IDENTIFICATION AND MARKING. DOT/FAA-originated material which contains information which requires protection against uncontrolled release shall be marked FOR OFFICIAL USE ONLY when necessary to ensure that all persons having access to the information are aware that it requires such protection. The marking FOR OFFICIAL USE ONLY shall include the notation in smaller print: "Public availability to be determined under 5 U.S.C. 552". Such marking shall be placed at the bottom of the outer cover, if any, the first page, and each succeeding page which contains FOUO information. Additional information is referenced in Appendix 10, Requirements For Safeguarding Sensitive But Unclassified Information.

a. If a document contains classified and FOUO information, a page containing both types of information shall be marked with the appropriate classification marking at the top and bottom of that page, but any page containing only FOUO information shall be marked FOR OFFICIAL USE ONLY at the bottom of that page.

b. Persons who have custody of material designated FOUO, whether marked or not, shall exercise due caution to ensure that the information is not made available to individuals who do not have a need to know.

c. During nonduty hours, FOUO material shall be kept in out-of-sight storage. This is only if access to the building or area is controlled by a guard force. In buildings without guard protection and access controls, the material shall be stored in locked desks or locked file cabinets.

d. All FOUO information is not equally significant. Some is more sensitive than others. Further, the importance of a specific FOUO item may vary in relation to time or as other developments may affect it. Personnel who have primary control of this type of information should consider affording a higher degree of protection to individual FOUO items when the sensitivity of the item would warrant more positive safeguards.

644.-699. RESERVED.

CHAPTER 7. ACCESS, DISSEMINATION, AND CONTROL OF CLASSIFIED NATIONAL SECURITY INFORMATION

SECTION 1. ACCESS TO CLASSIFIED INFORMATION

700. POLICY. In accordance with the provisions of E.O. 12958 and Information Security Oversight Office (ISOO) Directive Number 1, classified national security information may be released only to persons who have an official need for the information and only after they have been determined by properly designated authorities to be trustworthy for the classification level to be disclosed and have been issued a formal security clearance. The mere fact that an individual is employed by the FAA or another department or agency of the Government, or is a member of the armed forces, does not mean that she/he has been cleared for access to classified information. No one has a right to have access to classified information solely by virtue of rank or position. A Standard Form (SF) 312, Classified Information Non-Disclosure Agreement, shall be executed prior to granting access to classified information.

701. SECURITY CLEARANCE. No person shall be permitted access to classified information until a determination has been made of that person's trustworthiness. This determination, referred to as a security clearance, shall be based on an investigation in accordance with requirements specified in the latest edition of Order 1600.1, Personnel Security Program. The clearance data shall be entered into and retrieved from the Consolidated Personnel Management Information System (CPMIS) by the servicing security element (SSE). The security clearance defines the highest level of classified information to which the individual may be authorized access.

a. The latest edition of Order 1600.1 establishes policies, standards, procedures, and designated authorities for issuance and withdrawal of security clearances for FAA personnel.

b. Persons who are cleared for access to classified information at one level may, upon verification of operational need, be granted access to classified information at lower levels.

c. The number of people cleared and granted access to classified information shall be the minimum number consistent with operational requirements and needs.

702. NEED-TO-KNOW PRINCIPLE. In addition to possessing a valid security clearance for access to classified information, an individual must have an official verifiable need to know in connection with the performance of his/her official duties. The need-to-know principle is applicable in all cases, to include those instances in which the prospective recipient of the classified information is another Federal agency, a defense contractor, a foreign government, or another organization.

703. RESPONSIBILITY FOR DETERMINING NEED-TO-KNOW AND CLEARANCE.

a. Access to certain types of classified information may require special authorization and additional controls. Sensitive Compartmented Information (SCI) is an example of classified information where special access and clearance requirements apply.

b. The final responsibility for determining whether an individual's official duties require access to classified information and whether or not the individual has the appropriate security clearance rests with the individual who has possession, knowledge, or control of the information.

c. Supervisors disseminating classified information to employees or other persons under their jurisdiction are responsible for complying with the provisions of this order to include adherence to requirements for clearance, need to know, safeguarding, accountability, and control.

d. Material assigned a security classification shall not be released to an employee or other person for private use (personal, commercial, or as background material) even if the individual was partly or solely responsible for producing the material.

e. Before approving the release of classified information to a person who serves in more than one capacity, such as a contractor employee who is also a private consultant, the releasing official shall determine which capacity the intended recipient is acting in, and shall follow the release and clearance procedures for the appropriate category. If there is doubt concerning the appropriate course of action, the classified information account custodian (CIAC) or the SSE should be consulted prior to releasing the information.

f. Individuals who verbally disclose classified information are responsible for ensuring that the recipients have the proper security clearance and for advising the recipients of the security classification level of the information. In addition, it is the responsibility of the person or persons disclosing the classified information to ensure that the environment in which the discussion takes place is suitable for such discussions. Unless a conference room or other facility that has been specifically approved for discussion of classified information is available, the individual responsible for the information should consult with the SSE before entering into any discussion of classified information within an unapproved environment.

704. CONTINUOUS EVALUATION OF ELIGIBILITY AND ADMINISTRATIVE ADJUSTMENT OR TERMINATION OF SECURITY CLEARANCE. Supervisors shall continually evaluate information regarding persons who have been granted security clearances to ensure that the criteria defined in the latest edition of Order 1600.1 continue to be satisfied.

a. A security clearance shall be administratively terminated when an individual no longer requires access to classified information in the performance of his/her official duties.

b. When an individual no longer needs access to a particular level of classified information, the clearance shall be adjusted to the proper classification level required for the performance of official duties. For example, if an FAA employee no longer requires access to SECRET material in his or her job, but does require access to CONFIDENTIAL material, the clearance level shall be adjusted accordingly from SECRET to CONFIDENTIAL.

c. Under the conditions cited in paragraphs 704 a and b, an action to terminate or adjust a security clearance administratively shall be taken without prejudice to the individual's future eligibility for a security clearance.

705. PERFORMANCE PLANNING AND CRITICAL OUTCOMES AND EXPECTATIONS.

a. Performance Plan. Supervisors shall prepare an appropriate performance plan for employees who have been granted a security clearance (e.g., the employee understands and complies with FAA security orders pertaining to the safeguarding, accountability, and control of classified information).

b. Critical Outcomes and Expectations. The safeguarding of classified information shall be listed as a critical outcome and expectation in the performance plan for all FAA employees whose official duties and responsibilities require them to have a security clearance.

706.-710. RESERVED.

SECTION 2. DISSEMINATION OF CLASSIFIED INFORMATION WITHIN THE EXECUTIVE BRANCH

711. CLASSIFIED INFORMATION ORIGINATED BY DOT ACTIVITIES. Classified information originated by DOT activities may be disseminated to other departments and agencies of the executive branch when necessary for the conduct of official business.

712. CLASSIFIED INFORMATION ORIGINATED BY OTHER DEPARTMENTS OR AGENCIES. Classified information originated by another department or agency and furnished to the FAA shall not be distributed outside the FAA without the prior consent of the originating department or agency. This restriction also applies to distribution to cleared FAA contractors who require the information in the performance of FAA contracts.

713.-718. RESERVED.

SECTION 3. DISSEMINATION OF CLASSIFIED INFORMATION OUTSIDE THE EXECUTIVE BRANCH

719. GENERAL REQUIREMENTS. Classified information under the control of the FAA shall not be disseminated outside the executive branch without the specific authorization of ACS-1. The following additional requirements apply:

a. Marking. Classified information released outside the executive branch shall be appropriately marked in accordance with provisions of this order.

b. Responsibility for safeguarding. Offices which release classified documents are responsible for ensuring that the recipients can provide adequate physical safeguards.

720. DISSEMINATION OF CLASSIFIED INFORMATION TO THE CONGRESS. Provided FAA policies and procedures regarding legislative matters are met, classified information may be disseminated to Congress as authorized by the Administrator. Classified information shall be reviewed specifically, prior to release, to ensure that the classification is still valid. Congress includes members, committees, subcommittees, and staffs.

a. FAA personnel who appear as witnesses before congressional committees, or who meet with staff representatives, shall obtain prior authorization before disclosure of classified information.

b. An FAA employee who is appearing as a witness before a congressional committee and is asked to disclose classified information which has not been authorized for release shall respectfully state that he or she does not have authority to testify on the matter but will attempt to have the information furnished at a later date.

c. FAA employees appearing as witnesses before a congressional committee shall request that their testimony containing classified information be given in an executive session only, and that any record of such testimony be assigned the appropriate security classification level and not be permitted to appear in any document subject to public inspection or availability. An FAA employee shall obtain the assurance of a committee representative that everyone present at the time of the testimony has a security clearance equal to or higher than the security classification level of the information to be disclosed in the testimony.

d. Personal communications to Congress shall not include classified information.

721. DISSEMINATION OF CLASSIFIED INFORMATION TO THE GENERAL ACCOUNTING OFFICE (GAO). Representatives of the GAO who have official identification and whose security clearances for access to specific levels of classified

information have been confirmed by the SSE may be granted access to classified information when such information is relevant to the performance of the GAO's statutory responsibilities and duties.

a. The GAO usually provides advance notice to the FAA activities to be visited. Visit notification normally includes the purpose of the visit, the names of the GAO representatives, and a certification in writing by a GAO security officer or other authorized official of the security clearance of each representative.

b. The special credential issued by the Comptroller General is acceptable as identification. Each credential is serially numbered and bears the photograph and signature of the holder.

c. GAO requests for classified information that is TOP SECRET; that relates to sensitive tactical operations, intelligence, or communications security; or that another department or agency of the executive branch originated, shall be forwarded through ACS-1 to the Office of Security to determine if the information is relevant to the GAO's statutory responsibilities and for authorization for release or access.

d. When documents assigned a classification are furnished to the GAO representatives, the representatives shall be informed of the classification level of the information and of the need to provide adequate safeguards. The GAO has agreed to establish a security system equal to that required by the executive branch.

722. DISSEMINATION OF CLASSIFIED INFORMATION TO THE GOVERNMENT PRINTING OFFICE (GPO). Classified information, except TOP SECRET and unique information, including SCI, Special Access Program, and controlled cryptographic material, may be released to GPO plants for reproduction when FAA officials responsible for printing and reproduction coordinate with the appropriate SSE and the SSE determines that such release is necessary. The public printer has established policies and standards commensurate with those of the executive branch for the clearance of GPO personnel and for the safeguarding of classified information.

723. DISSEMINATION OF CLASSIFIED INFORMATION TO THE JUDICIARY. Every effort shall be made to prevent the disclosure of classified information during proceedings before civil courts or general courts-martial. If classified information becomes, or if it appears that it might become involved, the matter shall be referred immediately by ACS-1 to the Office of Security and Administrative Management, M-70 for referral to the General Counsel, OST. The General Counsel in consultation with M-70 shall provide the necessary advice and guidance.

724.-730. RESERVED.

SECTION 4. DISSEMINATION OF CLASSIFIED INFORMATION TO FOREIGN GOVERNMENTS, FOREIGN NATIONALS, AND INTERNATIONAL ORGANIZATIONS

731. RELEASE OF CLASSIFIED INFORMATION TO FOREIGN GOVERNMENTS. Except as provided for in E.O. 12958, ISOO Directive Number 1, Order DOT 1640.4C, and this section, classified national security information as a matter of principle and policy is not made available to a foreign national as an individual but is disclosed to his or her government. The foreign national receives the information in his or her capacity as an official or representative of the foreign government. By this means, the foreign government accepts responsibility for the security clearance of the individual and for the protection of the information.

732. RESPONSIBILITIES OF THE FAA. When the FAA is the proponent agency for release of classified information to a foreign government, the FAA shall, with the concurrence of DOT, make a clear determination that the benefits to the United States outweigh the disadvantages of disclosure. No release of classified information to a foreign national, foreign government, or international organization may be made by any FAA activity without the express prior written approval of ACS. Any proposed release of, or access to, classified information involving a foreign national which is not covered in this section shall be submitted to ACS through the appropriate SSE for consideration on a case-by-case basis.

733. RELEASE OF MILITARY CLASSIFIED INFORMATION. Policies governing the release to a foreign government of military information that is assigned a security classification are formulated by the National Military Information Disclosure Policy Committee.

734. RELEASE OF OTHER CATEGORIES OF NATIONAL SECURITY CLASSIFIED INFORMATION TO FOREIGN GOVERNMENTS. Release of certain other categories of classified information, including Restricted Data, intelligence, and communications security information, are made pursuant to policies established by the agency or interagency entity having cognizance over the classified information proposed for release. Often the determination as to which agency is the cognizant agency is difficult and involved and, in many cases, more than one department or agency may need to be consulted for approval.

735. RESPONSIBILITIES OF THE FOREIGN GOVERNMENT. The foreign government proposed as a recipient of U.S. classified information must officially ensure the U.S. Government that the information will be used only for official purposes, will be afforded protection at least equal to United States safeguarding requirements, and will not be released to any other person or nation without express permission of the United States, and that corporate or proprietary rights (if any) in the information will be respected.

736. RELEASE OF CLASSIFIED INFORMATION TO FOREIGN NATIONALS, FOREIGN GOVERNMENTS, AND INTERNATIONAL ORGANIZATIONS.

a. As noted in paragraph 732, no FAA activity may release classified information in any form to a foreign national, foreign government, or international organization without the express prior written approval of ACS. This section deals only with the safeguarding and controlled release of classified information. Other FAA and DOT directives pertaining to international relations should also be consulted. A U.S. citizen who is acting as a representative of a foreign government or organization, while not a "foreign national," is regarded as a "foreign entity" and is subject to all restrictions on dissemination of classified information that are applicable to foreign nationals.

b. The provisions of this section apply to all situations wherein a foreign national or foreign entity may gain access to classified information in the custody of the FAA. These situations include, but are not limited to, visits of FAA personnel to foreign countries and FAA employee participation with foreign nationals in exchange missions, conferences, meetings, and symposia.

c. To avoid embarrassment, FAA personnel should use care, good judgment, and avoid firm invitations or commitments to foreign nationals and foreign entities which may involve access to classified information until such access is expressly approved by the appropriate authorities and ACS. The fact that another department or agency may have sponsored or approved a foreign national or foreign entity visit in the form of granting a visit clearance for that agency does not authorize access to classified information in the custody of the FAA.

737. FOREIGN NATIONAL EMPLOYEES. In rare instances, an FAA organization may wish to hire a foreign national as an employee. In these cases, Human Resource Management Divisions (HRMD) shall follow appropriate DOT and FAA orders regarding the hiring of persons who are not U.S. citizens. However, if the foreign national will require access to classified information in order to perform his or her duties, the following procedures apply:

a. Request for authorization to release classified information. The employing office shall submit a request through the SSE and ACO-1 to ACS-1 for a determination as to whether the necessary classified information may be released to the prospective employee, subject to the granting of a Limited Access Authorization. The request shall identify precisely the classified information that the office intends to release to the foreign national. In making its determination, ACS shall use the same criteria it would use to determine whether or not the information could be released to the government of the country of which the individual is a citizen.

b. Applicants. If a foreign national is an applicant for a position which will require access to classified information, the HRMD shall make no offer of employment to that

individual unless ACS-1 has approved the release of the necessary classified information to that person, should he or she be employed and be granted the necessary authorization or clearance.

c. Processing for a limited access authorization or a security clearance. If ACS-1 determines that the specified classified information is releasable to the foreign national, the employing office shall then submit a request for either a limited access authorization or a security clearance. A foreign national who is not an immigrant alien is not eligible for a security clearance. An immigrant alien, a person lawfully admitted to the United States under an immigration visa for permanent residence, may be granted a clearance, but only under special compelling circumstances warranting a broader need to know. M-70 is authorized to grant limited access authorizations and security clearances to persons who are not U.S. citizens. This authority is not further delegated. The latest edition of Order 1600.1 specifies the procedures for obtaining these authorizations and clearances.

d. Restrictions. FAA activities shall only permit the foreign national employee access to that classified information which ACS has authorized for release. The office or activity manager shall establish, with the approval of the SSE, procedural controls, to screen all classified information furnished to the foreign national employees effectively.

738. ACCESS TO CLASSIFIED INFORMATION BY FOREIGN NATIONAL CONSULTANTS OR CONTRACTORS. Foreign national consultants or contractors requiring access to classified information shall comply with the requirements of E.O. 12829 and E.O. 10865, as amended. Any questions in this area should be addressed to ACO-400 through the SSE.

739. APPLICATION FOR OFFICIAL VISITS BY FOREIGN NATIONALS TO FAA ACTIVITIES WHERE ACCESS TO CLASSIFIED INFORMATION MAY BE INVOLVED. When a request for foreign nationals to visit an FAA facility involves possible access by those nationals to classified information, the manager of the FAA office or activity sponsoring the request is responsible for submitting the application request through appropriate channels to ACO-400 at least 30 working days in advance of the proposed visit. An information copy of the request shall be provided to the appropriate SSE. In the case of a civilian or military representative of a foreign government, application may be made by a civilian or military attache of the mission of the country concerned. For all other foreign nationals or foreign entities, application shall be made by the Chief of Mission (ambassador, minister, etc.) of the country concerned. Applications shall be typed and shall contain the following information concerning the proposed visit:

a. Full name, grade, title, and position.

b. Nationality; date and place of birth; and, if the individual is a civilian, passport number.

c. Name of employer or sponsor (if other than the government making application).

d. Name and address of each FAA facility to be visited.

e. Date, time, and estimated duration of each visit.

f. Purpose for the visit. Describe in detail, including the estimated degree and level of access to classified information that will be required.

g. Security clearance status of the visitor with his or her own government.

h. If available, the names of the individuals to be visited.

i. A certification that the visitor has been subjected to appropriate screening and does not constitute a security risk to the United States, and that the visit and visitor are officially sponsored by his or her government which has officially cleared him or her to receive information for the stated purpose. The certification shall further state that responsibility for the security of the information obtained is officially accepted by the visitor's government, that all information obtained will be used for official purposes only, that it will not be released to any other person or nation without the express consent of the U.S. Government, and that corporate or proprietary rights involved, patented or not, will be respected and protected.

740.-745. RESERVED.

SECTION 5. RELEASE OF CLASSIFIED INFORMATION TO HISTORICAL RESEARCHERS

746. SCOPE. The provisions of this section apply only to persons who are conducting historical research as private individuals or under private sponsorship and do not apply to research conducted under government contract or sponsorship. The provisions of this section are applicable only to situations where the classified information concerned in whole or in part was originated by DOT or by DOT contractors, or where the information, if originated elsewhere, is in the sole custody of the DOT. Under these conditions, with the approval of ACS, historical researchers may have access to classified information provided that it can be clearly shown that access to the information will be in the interest of the national security and that the person to be granted access is trustworthy. Persons who request access to classified material originated in another agency, or to information under the exclusive jurisdiction of the National Archives and Records Administration (NARA), should be referred to the other agency or to NARA.

747. PREPARATION OF REQUEST FOR ACCESS TO CLASSIFIED INFORMATION. When a request for access to classified information for the purpose of historical research is received, it will be referred to the appropriate SSE. The SSE will obtain from the applicant a completed SF 86, Questionnaire for Sensitive Positions, and an FD 258, FBI Fingerprint Chart. The following information shall also be obtained:

a. A statement in detail justifying the need for access to classified information, including identification of the kind of information desired and the organization(s), if any, sponsoring the research.

b. A written statement that is signed, dated, and witnessed with respect to the following:

(1) The individual seeking access understands that any classified information that he or she receives affects the national security of the United States and agrees to abide by FAA regulations issued to safeguard national security classified information.

(2) The individual agrees to protect information which has been determined to be proprietary or privileged in nature and not eligible for public dissemination.

(3) The individual agrees not to reveal any classified or privileged information except as specifically authorized in writing by the FAA, and agrees not to use the information for purposes other than those set forth in his or her application.

(4) The individual authorizes the SSE to review his or her notes and manuscript for the sole purpose of determining that no classified material is contained therein.

(5) The individual understands that failure to abide by the conditions of this statement will constitute sufficient cause for cancellation of his or her access to classified information, and for denying him or her any future access.

(6) The individual is aware of and understands that the provisions of Title 18, U.S.C., Crimes and Criminal Procedures of the Internal Security Act of 1950, as amended; and of Title 50, U.S.C., prescribe criminal penalties under certain circumstances for the unauthorized disclosure of information concerning the national security and for the loss, destruction, or compromise of such information. See Appendix 6, Extracts from U.S.C. Title 18 and Title 50.

(7) The individual acknowledges that this statement is made to the U.S. Government to enable it to exercise its responsibilities for the protection of information affecting the national security, and that any material false statement which he or she makes knowingly and willfully will subject him or her to the penalties of Title 18, U.S.C. See appendix 6.

748. PROCESSING REQUESTS FOR ACCESS TO CLASSIFIED INFORMATION.

a. The SSE shall submit to the Office of Personnel Management the forms the prospective historical researcher provided and shall request a National Agency Check with Inquiries (NACI) investigation. Order 1600.1 contains the procedures for initiating the NACI.

b. Upon receipt and review of the completed NACI, the SSE shall make a determination as to whether or not the applicant's access to the classified information would be clearly consistent with the interests of national security and whether the person to be granted access is trustworthy. If necessary, the SSE may conduct or request further investigation before making such a determination.

c. If access is being requested to TOP SECRET, intelligence, or cryptographic information, a complete Single Scope Background Investigation (SBI) is required. An SBI shall not be requested, however, until the matter has been referred through ACS-1 to M-70 for a determination as to adequacy of the applicant's justification and the need for the consent of other agencies as required. When an applicant's research might extend to material originating in the records of another agency, approval shall be obtained from the other agency prior to the individual being granted access.

d. Before a decision is made to deny access, the matter shall be referred by the SSE through ACS-1 to M-70 for review and submission to the Secretary of Transportation for final denial.

749. DURATION OF ACCESS APPROVAL. Approvals for access shall be valid for the duration of the current research project, but unless renewed, for no longer than 2 years from the date of issuance. If the individual makes a subsequent request for access within 1 year from the date of completion of the current project and the need-to-know, trustworthiness, and national interest factors upon which the original access was granted remain unchanged, access may again be granted with the approval of the SSE without obtaining a new NACI. If more than 1 year has elapsed, a new NACI shall be obtained. The SSE shall promptly advise ACO-400 of all approvals of access granted under these conditions.

750. RESTRICTIONS ON ACCESS TO CLASSIFIED INFORMATION. An applicant shall be allowed access only to that classified information which is directly pertinent to his or her project. The following requirements apply:

a. He or she may review files or records containing classified information only in offices under the control of DOT.

b. Procedures shall be established wherever possible to identify and confirm specific classified information to which the individual is given access.

c. The individual shall be briefed by the SSE or CIAC on local procedures established to prevent unauthorized access to the classified material while in his or her custody. The briefing shall include instructions for the return of the classified material, for secure storage at the end of the daily working period, and for the control of any notes made until they have been reviewed by the SSE.

751.-755. RESERVED.

SECTION 6. DISSEMINATION OF CLASSIFIED INFORMATION TO FORMER PRESIDENTIAL APPOINTEES, CONTRACTORS, AND OTHERS

756. DISSEMINATION OF NATIONAL SECURITY CLASSIFIED INFORMATION TO FORMER PRESIDENTIAL APPOINTEES. Persons who previously occupied policymaking positions to which they were appointed by the President may be granted access to classified information or material which they originated, reviewed, signed, or received while in public office, subject to the following provisions of this paragraph.

a. The appropriate authority has determined that such access is clearly consistent with the interests of the national security.

b. The individual requesting access agrees to safeguard the classified information, to ensure that it is not further disseminated, and to authorize a review of his or her notes by the SSE to ensure that classified information is not contained therein.

757. DISSEMINATION OF CLASSIFIED INFORMATION TO CONTRACTORS. Subject to the provisions of E.O. 12829 and E.O. 10865 as amended, and DOD 5220.22M, National Industrial Security Program Operating Manual (NISPOM), classified information may be disclosed to appropriately cleared DOT contractors, subcontractors, bidders, and grantees, and to appropriately cleared contractors of other government agencies, provided that access to the classified information is necessary to perform the contract and that FAA has received written certification that the necessary personnel have the required security clearances.

758. DISSEMINATION OF CLASSIFIED INFORMATION TO NATIONAL DEFENSE EXECUTIVE RESERVISTS (NDER). For the purpose of dissemination, members of the DOT NDER program are considered to be in the same category as employees. Classified information may be disclosed to DOT NDER's for which they have a need-to-know and provided the appropriate security clearances have been issued pursuant to the provisions of the latest edition of Order 1600.1. However, classified information shall not be physically released to the custody of NDER's except when such requests

are approved by the Director of Emergency Transportation, Research and Special Programs Administration, DET-1, and the release is in accordance with procedures established by the latter after consultation with M-70.

759. DISSEMINATION OF NATIONAL SECURITY CLASSIFIED INFORMATION TO THE NEWS MEDIA. No person in the FAA shall discuss classified information with or provide it to the news media. All contacts with the news media involving classified information, whether written or oral, shall be referred through ACS-1 to M-70. ACS shall be consulted before any commitment to or understanding with the individual or entity has been reached.

760. DISSEMINATION OF NATIONAL SECURITY CLASSIFIED INFORMATION TO OTHER RECIPIENTS. Proposed releases of classified information to persons not categorized in the preceding paragraphs shall be referred to ACO-400 for approval and determination of limitation on release, if any. ACO-400 shall provide guidance with regard to measures necessary to ensure the trustworthiness of the proposed recipient. ACO-400 shall be consulted before any commitment to or understanding with the individual or entity has been made.

761. DISSEMINATION OF CLASSIFIED INFORMATION THROUGH MEETINGS. Organizations which host or convene a conference, symposium, seminar, exhibit, or scientific and technical gathering (hereinafter referred to as a meeting) shall ensure that security measures are taken that are appropriate to the circumstances. Requirements include but are not limited to the following:

a. Meeting arrangements should be coordinated with the SSE to ensure that concerns relevant to the safeguarding of classified information are addressed.

b. All persons attending the meeting shall be properly cleared and have a need for the classified information to which they will have access. In this regard, all attendees may not have a need for all of the information to be presented, particularly at a meeting covering a wide range of topics. In such instances, the meeting's agenda should allow for limiting attendance at those portions where classified information will be discussed only to those persons who need to know it. Doing so will eliminate the need for clearances for any attendees who do not need access to the classified information.

c. Attendees at sessions where classified information may be discussed shall be positively identified before being admitted to the meeting room.

d. Persons who present classified information shall be advised of any limitation on their presentations which may be necessary because of the level of clearance or need-to-know of certain members of the audience. The speaker is responsible for seeking such guidance and for keeping his or her disclosures within the prescribed limits.

e. Notes, minutes, summaries, recordings, proceedings, reports, etc., on the portions of the meetings dealing with classified information shall be safeguarded and controlled throughout the duration of the meeting. Such material shall be forwarded to attendees by secure means at the conclusion of the meeting rather than being hand-carried by them from the meeting site (except for local attendees).

f. Physical and technical security controls shall be established as appropriate to the classification and sensitivity of the information to be discussed. Because of the security hazards inherent in the use of any normally public meeting place for the presentation or discussion of classified information, classified meetings or classified sessions of a meeting shall, whenever possible, be held only on a U.S. Government installation or at a cleared contractor facility. Exceptions to this provision for FAA-sponsored meetings must be approved by the SSE prior to implementation.

g. The FAA official or contractor official responsible for the classified meeting shall designate an appropriately cleared individual in writing to serve as a security point of contact during the meeting. This individual shall be responsible for ensuring that area security and administrative security procedures and safeguards are carried out.

762.-770. RESERVED.

SECTION 7. CONTROL OF NATIONAL SECURITY CLASSIFIED INFORMATION

771. ACCOUNTING PROCEDURES. Through effective accounting procedures, it is possible to trace the movement of classified information and material, identify persons afforded access, limit dissemination, retrieve documents promptly, detect the loss of information or material, and prevent excessive production and reproduction of documents.

772. REQUIREMENT FOR ESTABLISHMENT OF A SECURITY CONTROL POINT (SCP). An SCP shall be established within each FAA activity which has a requirement to handle classified information. The SCP shall be under the supervision of an appropriately cleared CIAC and one or more ACIAC's. The SCP shall process all incoming and outgoing classified material for the office or activity. The CIAC and the ACIAC's shall be designated in writing in accordance with this order.

773. EXCEPTIONS FOR COMMUNICATIONS SECURITY (COMSEC), SPECIAL INTELLIGENCE, REGISTERED PUBLICATIONS SYSTEMS, RESTRICTED DATA, NATIONAL SECURITY COUNCIL INTELLIGENCE INFORMATION, AND OTHER UNIQUE MATERIAL.

a. National security classified materials in these categories that are accountable under other control systems shall be received and accounted for by the respective

custodians appointed for these purposes who shall operate in conformance with the regulations prescribed for the particular type of information concerned. COMSEC-related classified documents that are not accounted for in the COMSEC Material Control System shall be controlled as prescribed for other classified material (e.g., National Telecommunications and Information System Security Instructions (NTISSI), and National Telecommunications and Information Systems Security Policy (NTISSP)).

b. National Security Council (NSC) information refers to classified information contained in: (1) any document prepared by or intended primarily for use by the NSC, its interagency groups, or its associated committees and groups; and (2) deliberations of the NSC, its interagency groups, or its associated committees or groups. The DOT holds the number of persons having access to NSC information to the absolute minimum consistent with efficient operations of the NSC system, and strictly controls document dissemination and reproduction in accordance with existing laws. A special cover sheet prepared and distributed by the NSC will be affixed to all NSC documents.

774. SCP CONTROL OF CLASSIFIED MATERIAL THAT IS HAND CARRIED TO OR FROM AN ACTIVITY. Personnel of an activity who receive TOP SECRET or SECRET material directly from a visitor, or who bring such material back to their office as a result of their visiting another activity, shall immediately have the material processed by the SCP. TOP SECRET material shall be processed by the Top Secret Control Officer (TSCO) or the Alternate Top Secret Control Officer (ATSCO). Similarly, personnel who release SECRET material directly to an authorized visitor or to another activity as a result of their visiting, shall obtain a receipt which shall be provided to the SCP. FAA personnel shall coordinate with the SCP CIAC prior to any such transfer. FAA personnel returning to their facility with classified material shall ensure that the classified material is properly marked and packaged while in transit.

775. FUNCTIONS OF THE SCP. The primary functions of the SCP in an office or activity include the following:

a. The SCP assigns document control numbers to each new item of SECRET material received by the office or activity and maintains the accountability records for SECRET information. Please refer to paragraph 777 of this chapter for additional information on TOP SECRET control requirements.

b. The SCP CIAC verifies the clearance status of recipients of incoming classified information and ensures that appropriate safeguards are provided before transferring the information to their control.

c. The SCP CIAC or ACIAC receives unopened all incoming registered and certified mail for the office, activity, or facility and inspects the mail to detect any evidence of tampering before opening. Upon opening any mail containing classified material, the CIAC matches the actual contents of the package with the enclosed receipt.

d. The SCP CIAC signs and returns to the sender receipts enclosed in classified transmittals.

e. The SCP CIAC ensures that the appropriate secure methods of transmission (except telecommunications) are selected for the transmission of classified material in accordance with the provisions of this order.

f. The SCP CIAC ensures that receipts are obtained for SECRET material sent from or within the office, activity, or facility. CONFIDENTIAL material that is sent by First Class mail may be covered by receipts at the option of the sender.

g. The SCP CIAC shall destroy classified information or arrange for its destruction in accordance with the requirements of Chapter 12, Destruction and Disposal of Classified Information.

776. REQUIREMENT FOR MAINTAINING FAA FORM 1600.35, CLASSIFIED DOCUMENT REGISTER. FAA Form 1600.35, Classified Document Register, for SECRET material shall be established, maintained, and kept current at the SCP. The register shall be used to log in and account for SECRET classified information in accordance with the requirements listed in this paragraph.

a. When SECRET material is received at the office, activity, or facility, the CIAC shall assign a log control number. The control number and other pertinent information shall be entered on the FAA Form 1600.35 for accountability purposes.

b. When SECRET material is generated, reproduced, or destroyed within an office, activity, or facility, the CIAC shall make the appropriate notation on the FAA Form 1600.35.

c. When SECRET material is transferred from one office to another within an activity, or when it is dispatched outside an activity on a permanent or temporary basis, the CIAC shall enter this information on the FAA Form 1600.35.

777. CONTROLS FOR TOP SECRET CLASSIFIED INFORMATION. Each office, activity, or facility having a requirement to handle TOP SECRET material shall appoint in writing, a TSCO and an ATSCO. The TSCO may be the same individual holding the position of SCP CIAC. If the TSCO is a different individual from the SCP CIAC, he or she shall receive, log in, retain permanent custody of, account for, and dispatch, all TOP SECRET material for the office, activity, or facility. The TSCO shall be responsible for maintaining all the accountability records and controls this order requires for TOP SECRET material, including those listed in this paragraph.

a. The TSCO shall affix a disclosure record (DOT F 1600.32) to each TOP SECRET document. This record shall reflect the document title, the name of all individuals who have had access to the document, including those to whom only oral disclosure has been made, and the date(s) of such access.

b. The internal and external transfer of TOP SECRET material shall be covered by a continuous receipt system, regardless of how brief the period of custody.

c. The original and all copies of TOP SECRET documents shall be numbered in series. Distribution records, receipts, and accountability records shall list the copy number as part of the document identification.

d. All TOP SECRET material shall be returned to the TSCO for overnight storage.

778. ACCOUNTABILITY INFORMATION TO BE ENTERED ON THE CLASSIFIED DOCUMENT REGISTER IN THE SCP.

a. The records maintained at the SCP for any document shall, as a minimum, reflect the following information:

(1) The date of receipt of the document and the date of origination.

(2) The title of the activity from which the document was received or which originated the document.

(3) A brief, unclassified description of the document.

(4) The assigned classification of the document.

(5) The date of any downgrading action, the date for declassification, or the date for review for declassification. Records shall be maintained in such a manner as to permit the CIAC to identify classified material immediately as it becomes downgraded or declassified or when it is eligible for a review for declassification.

(6) A document control number which the SCP CIAC has assigned.

(7) Information showing the disposition of the document, to include the date on which the document was destroyed, downgraded, declassified, or dispatched outside the office, activity, or facility.

b. An SCP may automate its control records. Such action must have the prior approval of ACO-400.

779. ACCOUNTABILITY RECORDS FOR CONFIDENTIAL MATERIAL. No accountability records need be established or maintained by the SCP for CONFIDENTIAL material; however, all incoming and outgoing CONFIDENTIAL material shall be processed through the SCP to ensure that the classification markings, packaging procedures, declassification guidance, and other security requirements are met.

780. RETENTION OF ACCOUNTABILITY RECORDS. Accountability records, FAA Form 1600.35 and DOT Form 1600.29, for TOP SECRET and SECRET material shall be retained for a minimum of 4 years after final disposition. At the end of this period, they may be destroyed. Existing accountability records for CONFIDENTIAL material established under previous executive orders may be destroyed.

781. CONTROL OF SECRET AND CONFIDENTIAL WORKING PAPERS. Working papers are documents, including drafts, notes, photographs, etc., accumulated or created to assist in the formulation and preparation of a finished document.

a. Working papers classified at the SECRET and CONFIDENTIAL level may be released within an office or activity for review and coordination without processing through the SCP provided the following conditions are met:

(1) The person responsible for the papers determines that the recipient has the appropriate clearance, the need to know, and the proper facilities for safeguarding the information.

(2) For SECRET working papers a receipt shall be prepared by the releasing office identifying the material. This receipt is to be signed by the recipient and the original retained by the releasing office CIAC with a copy to the recipient.

(3) The material shall either be destroyed within 30 days or returned to the releasing office. If SECRET working papers are retained by any office more than 30 days, the individual(s) responsible for the papers shall take them to the SCP to be entered into the classified document accountability system by the SCP CIAC.

b. The originator of a working paper that contains classified information at the SECRET or CONFIDENTIAL level is responsible for ensuring that the procedures listed below are followed.

(1) The document shall be dated at the time that it is created.

(2) The document shall be marked with the highest classification of any information it contains.

(3) The document shall be marked with downgrading or declassification instructions.

(4) The document shall be safeguarded in accordance with the security classification level assigned.

(5) The document shall be destroyed by the appropriate SCP CIAC when it has served its purpose.

(6) A document cover sheet (SF-703, SF-704, or SF-705), used as a shield to protect a classified document, shall be affixed to the top of the working paper and shall remain attached until the document is destroyed or placed in a GSA-approved storage container that has been approved by the SSE for the level of classification involved.

c. File folders used to store classified working papers shall be marked top and bottom, front and back, with the highest classification level of the material stored within the folder.

d. All SECRET and CONFIDENTIAL working papers that are transmitted outside an office, activity, or facility on a temporary or permanent basis shall be processed through the SCP.

782. DOCUMENT CONTROL STATION (DCS). In larger activities in which the SCP serves many offices, with the approval of the SSE, each office which has or will have custody of classified information shall establish a DCS under the supervision of a CIAC designated in writing in accordance with the provisions of this order. The DCS may be established organizationally at the office, service, division, or lower level, dependent upon the circumstances and the recommendation of the SSE. Where DCS facilities have been established for an office, the SCP shall release classified material intended for that office only to the DCS CIAC or other cleared persons in the office designated in writing by the office manager as authorized to receive classified materials from the SCP.

a. The DCS shall receive all SECRET and CONFIDENTIAL material that flows into or out of an office. TOP SECRET material shall be handled by the designated TSCO in accordance with the provisions of this order.

b. The DCS CIAC shall maintain a record or log of all SECRET material received in the office. The TSCO shall maintain a log for all TOP SECRET material received. The log shall also show the individual or section which has custody of the material.

c. A log is not required for CONFIDENTIAL material.

d. The DCS CIAC shall ensure that recipients of classified material are properly cleared and are familiar with the procedures for properly handling, safeguarding, and storing the classified material.

e. The SCP CIAC shall maintain a record of the identity and clearance status for each DCS CIAC, ACIAC, or other designated operator. The supervisor or manager having responsibility for the DCS shall provide this information to the SCP on DOT Form 1600.31, Document Control Station Establishment Authorization.

783.-799. RESERVED.

CHAPTER 8. STORAGE AND SAFEGUARDING OF CLASSIFIED INFORMATION

800. GENERAL. Classified material, when not in actual use and under the control of an appropriately cleared person, shall be stored and protected in accordance with this chapter. Storage facilities for classified information shall be approved in writing for the intended purpose by the SSE prior to being placed into operation.

801. STANDARDS FOR STORAGE EQUIPMENT. The General Services Administration (GSA) establishes and publishes uniform standards, specifications, and supply schedules for containers, vaults, and associated security devices and equipment suitable for the storage and protection of classified information. Cabinets, manufacturers, and prices of storage equipment approved by the GSA are listed in the Federal Supply Schedule (FSS) catalog (FSC GROUP 71-Part III). Copies of specifications and schedules may be obtained from any regional office of the GSA or through the SSE. Special problems or situations concerning security containers and associated security procedures should be addressed to the SSE.

802. TOP SECRET STORAGE. TOP SECRET material shall be stored in a GSA-approved security container that has been inspected and approved by the SSE. TOP SECRET material may, with the prior approval of ACO-400, also be stored in an approved Class A, B, or C vault, with supplemental controls. See Appendix 7, Construction Requirements for Controlled Areas.

803. TOP SECRET SUPPLEMENTAL CONTROLS. During nonworking hours, the following area (room, building, or structure) controls are required for TOP SECRET material.

a. Entry to the area in which the security storage container is located shall be controlled by a SECRET cleared, authorized employee or guard stationed to control access to the area or by a lock which has been approved for that purpose by the SSE and which provides reasonable protection against surreptitious entry.

b. The area in which the container is located, or the container itself, shall be equipped with an alarm system that meets the requirements of this order and that has been approved in writing by ACO-400.

804. SECRET AND CONFIDENTIAL MATERIAL STORAGE. SECRET and CONFIDENTIAL material may be stored in any manner approved for TOP SECRET.

805. SECRET SUPPLEMENTAL CONTROLS. During nonworking hours, the following area (room, building, or structure) controls are required for SECRET material. Entry to the area where the container is located shall be controlled by a SECRET cleared, authorized FAA employee or guard stationed to control access to the area or by a lock which has been approved by the SSE and provides reasonable protection against surreptitious entry.

806. CONFIDENTIAL STORAGE. CONFIDENTIAL material shall be stored in a GSA-approved security container in the same manner as TOP SECRET or SECRET material except that no supplemental controls are required.

807. SAFEGUARDING STORAGE CONTAINERS AND COMBINATIONS. Only a minimum number of authorized persons shall have knowledge of the combinations to the storage containers or have access to the information stored therein. Containers shall bear no external markings indicating the level of classified material authorized to be stored therein.

a. A record of the names and telephone numbers of persons having knowledge of the combinations shall be maintained as prescribed by this order.

b. Security containers, vaults, cabinets, and other authorized storage containers shall be kept locked when not under the direct supervision of an authorized person entrusted with the contents. Combination padlocks shall be placed inside an open container or secured to a hasp, drawer, or handle of the container to prevent substitution.

c. The combination shall be safeguarded in accordance with the highest classification of the material authorized for storage in the container. Protective measures need not be extended to superseded combinations.

d. To ensure positive locking of the security container or a security vault door equipped with a Group 1R-type combination lock or high security padlock, the individual locking the cabinet or door shall rotate the lock dial at least four complete turns in both directions.

e. Items of intrinsic value such as money, cameras, software, firearms, etc., shall not be stored in security storage containers used for the storage of classified information.

f. Casters for security storage containers are PROHIBITED.

g. Reversible OPEN-CLOSED signs shall be used on all security containers and vault doors to reflect the status of the locking device.

808. APPROVAL AND INSPECTION REQUIREMENT.

a. Approval. The SSE shall inspect the area designated for use in storing classified material and the containers in which the material is to be kept. Prior written approval of both the area and the container is required from the SSE before classified materials may be stored.

b. Inspection. When an office, activity, or facility, maintains a classified account, the SSE shall ensure that each scheduled physical security inspection and survey

include an assessment of the classified information account to ensure that the required safeguards and controls are being implemented. SSE inspections shall include but not be limited to the inspection of:

(1) The security storage container and controls.

(2) The overall area physical security and access controls.

(3) Classified document handling procedures and controls.

809.-814. RESERVED.

815. DAMAGE AND REPAIR OF APPROVED SECURITY CONTAINERS. Neutralization of lockouts or repair of any damage that affects the integrity of a security container approved for storage of classified information shall be accomplished only by appropriately cleared or continuously escorted personnel specifically trained in approved methods of maintenance and repair of containers.

a. An approved security container is considered to have been restored to its original state of security integrity if one of the following actions has been taken:

(1) All damaged or altered parts are replaced with manufacturer's replacement or identical parts.

(2) When a container has been drilled to neutralize a lockout, the drilled hole is repaired with a tapered case-hardened steel rod with a diameter slightly larger than the hole, and of such a length that when driven into the hole, there shall remain at each end of the rod a shallow recess of not less than 0.125 inch, nor more than 0.188 inch deep, to permit the acceptance of substantial welds, and be welded both on the inside and outside surfaces. The outside repaired drawer head shall then be puttied, sanded, and repainted in such a way that no visible evidence of its repair remains.

b. Approved security containers that have been drilled or repaired in a manner other than as described in paragraph 815a (2) shall not be considered to have been restored to their original integrity. The Test Certification Label on the inside of the locking drawer and the "General Services Administration Approved Security Container" label on the outside of the top drawer shall be removed from such containers.

c. An approved container may be repaired with welds, rivets, or bolts which cannot be removed or replaced without leaving evidence of entry. An approved container repaired in such a manner may be used only for the storage of CONFIDENTIAL material, or for SECRET material with supplemental controls, where approved by the SSE. A container that has been repaired using methods other than those described in this chapter shall not be used for storage of classified material.

d. Before a repaired container is returned to service, it shall be inspected and approved in writing by the SSE. The manager of the office or facility responsible for the container, or the container custodian, shall maintain a list of all approved security containers for which they are responsible which have sustained significant damage. Each container listed shall be identified by its location and a description of the damage. There shall also be on file a signed and dated certification, provided by the repairer, setting forth the method of repair used. The list and certification shall be retained for the life of the container and shall be available for review during recurring security inspections by the SSE. Each repaired container shall have a label posted on the inside of the top drawer to indicate the highest category of classified material which may be stored therein.

816. CONTROLLED AREAS. A controlled area is created by management when it is desired or required to limit or deny unauthorized personnel access to the area. The FAA uses two types of controlled areas--Closed and Restricted. The office or facility manager having overall responsibility for the safeguarding of classified material shall coordinate with the SSE to agree mutually upon the need to establish controlled areas and on the type and extent of such areas.

a. Closed Area. Areas in which classified information is processed, handled, transmitted, or stored on a regular basis shall be designated as a Closed Area. A Closed Area must meet the construction requirements of appendix 7 and unescorted access shall be limited to individuals who possess the appropriate security clearance and who have a valid need to know for the information contained within the area. The Closed Area designation is to be applied only for the purpose of safeguarding classified information and shall not be used for any other purpose. Examples of areas that shall be designated as Closed areas include, but are not limited to, Security Control Points and secure on-line telecommunications centers. Closed Areas shall be clearly identified by Closed Area signs affixed to all accessible perimeter surfaces and shall be secured in accordance with this order at all times when not attended.

b. Restricted Area. The term Restricted Area is used throughout the FAA and the Government in general to indicate that access to an area so designated is limited to authorized persons who require access in the performance of their official duties. Although intended for application in a variety of operational areas, the Restricted Area designation may be considered as a means to enhance but not substitute for required classified information safeguards.

c. Disestablishment of Controlled Areas. A controlled area shall be disestablished when there is no longer any need for the controls (for example, all classified information is removed from the area for delivery to the customer), and there is no anticipated future need to reactivate the area for safeguarding classified material.

817. SAFEGUARDING REQUIREMENTS FOR CLOSED AREAS. Closed areas shall be separated from adjacent areas by a physical barrier constructed of materials that provide protection against unauthorized access to, or removal of, classified material. Like other storage equipment, closed areas are used, in part, to provide reasonable deterrence against physical penetration and prevention of surreptitious entry commensurate with the classification level of the information requiring protection. Closed Areas shall meet the construction requirements of appendix 7, and the latest edition of Order 1600.6, FAA Physical Security Management Program. There are no specific construction requirements for Restricted Areas.

a. A Closed Area shall be designated and marked "CLOSED AREA." A Restricted Area shall be designated and marked "RESTRICTED AREA."

b. Closed areas shall be physically configured, in conjunction with internal personnel controls and procedures, in a manner that reasonably minimizes the possibility that unauthorized personnel can transgress the area undetected. Personnel within the area are responsible for challenging all persons who may lack appropriate access authority, regardless of the nature of perimeter controls in use.

818. CLOSED AREA CONTROL DURING WORKING HOURS. The controls described in this paragraph are predicated on a situation where classified information is considered to be accessible to anyone entering the area.

a. TOP SECRET Material. Admittance shall be continuously controlled by a TOP SECRET cleared guard posted at the entrance, unless an approved automated access control device has been approved by the SSE for use in lieu of a guard. When an approved access control device is not used, the employee or guard designated to control the entrance shall be required to open the entrance, remain at the entrance while it remains open, supervise the passage of material or authorized personnel through the entrance, and to close the entrance immediately thereafter.

b. SECRET or CONFIDENTIAL Material. Admittance shall be continuously controlled by an appropriately cleared employee or guard stationed to monitor entrance to the area, unless an approved automated access control device, or an approved electric, mechanical, or electromechanical device has been approved by the SSE for use in lieu of an employee or guard. When an approved access control device is not used, the employee or guard is required to perform the same functions detailed in paragraph 818a above.

819. CLOSED AREA CONTROLS DURING NONWORKING HOURS. Admittance to a Closed Area shall be controlled by locked entrances and exits secured with a GSA-approved, changeable combination lock. However, doors secured from the inside with a panic bolt (for example, actuated by a panic bar), a dead bolt, a rigid wood or metal bar, or other means approved by the SSE, will not require additional locking devices. Safety and fire requirements shall be adhered to when selecting and installing locks and other protective measures.

a. If TOP SECRET material is stored in a Closed Area, the following supplemental controls are required:

(1) The Closed Area shall be alarmed with an approved intrusion detection system that has been approved in writing by the SSE. The system shall include protection of movable and fixed openings as well as volumetric protection for the area.

(2) The area shall be thoroughly checked at the end of the working hours, by the last person leaving, to ensure area integrity and that no individual remains inside.

(3) A record including the signature of the person securing the area, and the time secured, shall be posted on the interior side at the door.

(4) A log shall be posted on the exterior of each door, and the TSCO or his or her designated representative shall be required to sign and indicate the time checked, certifying that the door was checked and found to be locked.

b. If SECRET or CONFIDENTIAL material only is stored in a closed area, alarm systems are not required, however, the area check and control procedures described in paragraph 819a, shall be followed whenever possible.

820. RESTRICTED AREA CONTROLS. In areas such as open offices where classified documents are used on a regular basis, it may be impossible or impractical to comply with CLOSED AREA construction requirements for the entire area. Under these conditions, RESTRICTED AREA signs shall be used for the areas concerned to reduce to a minimum the volume of unauthorized personnel who access the area. The RESTRICTED AREA designation is a personnel control measure and not a substitute for the CLOSED AREA designation or safeguarding requirements. All other requirements of this order for the safeguarding, handling, and storage of classified information apply.

821. STORAGE OF CLASSIFIED MATERIAL IN VAULTS. Storage of classified material in approved vaults is an alternative to storage in approved security containers under certain conditions. Normally, FAA facilities will not have approved vault storage facilities for classified material. In the event, however, that such storage is available and the manager of the office or facility having the responsibility for the classified information desires to use the vault for storage, he or she shall coordinate with the SSE to determine the requirements that must be met. As a minimum, coordination with the SSE and the prior written approval of ACO-400 shall be required before vault storage is decided upon.

822. STORAGE OF CLASSIFIED MATERIAL IN STRONGROOMS. The requirements for coordination with the SSE and prior approval of ACO-400 are the same for strongroom storage proposals as for vaults.

823. SUPERVISION OF KEYS AND LOCKS. Where the use of key-operated padlocks in the safeguarding of classified material has been approved by the SSE, the procedures established shall be subject to the key and lock control requirements of the latest edition of Order 1600.6, to include the following:

a. A key and lock custodian shall be appointed to ensure proper custody and handling of keys and locks used for the protection of classified material.

b. A key and lock control register shall be maintained to identify keys for each lock and their current location and the individual responsible for their custody.

c. Keys and locks shall be audited each month.

d. Keys shall be inventoried at each change of custody.

e. Keys shall not be removed from the premises.

f. Keys and spare locks shall be protected at a level equivalent to the level of classified material involved.

g. Locks shall be changed or rotated at least annually and shall be replaced after loss or compromise of their operating keys.

h. Making master keys is prohibited.

824. APPROVED ALARM SYSTEM. This paragraph specifies the minimum standards for approved Intrusion Detection Systems (IDS) equipment, installation, and operation when used for safeguarding TOP SECRET information.

a. Central station. The IDS shall be connected to and monitored by a central control station.

b. Alarm. The IDS shall provide for the protection of all fixed and movable openings, and in addition, shall provide for volumetric protection. An alarm shall result in an audible and visual alarm signal capable of alerting a response force and directing them to the location of the alarm. Response time to the alarm shall not exceed 15 minutes.

c. Approval. Approval of the SSE is required before initiating installation of an IDS to meet the requirements of this paragraph. For TOP SECRET material, the proposed IDS must also have the prior approval of ACO-400.

d. Central Station Control. The central control station may be located at the FAA facility, at a military or GSA monitor facility, or at a cleared commercial central station listed with Underwriter Laboratories Incorporated (UL).

(1) For a military or GSA central station, trained alarm monitors cleared to the SECRET level shall be in attendance at the central station at all times when the IDS is in operation.

(2) For an FAA proprietary central station, trained guards, cleared to the SECRET level and sufficient in number to be dispatched immediately to investigate each alarm, shall be available at all times when the IDS is in operation.

(3) For a commercial central station, personnel dispatched shall be cleared only if they have the ability and responsibility to access the area or container(s) housing classified material.

(4) A signal shall be maintained at the central station to show whether or not the system is in working order and to indicate tampering with any element of the system. If repairs are required, they shall be made as soon as practical. Until repairs are completed, periodic patrols shall be instituted during nonworking hours unless an employee, cleared for SECRET, is stationed at the alarmed site.

(5) Guards dispatched by a commercial central station to an alarm shall remain on the premises until a designated cleared representative of the facility arrives or for a period of not less than 1 hour, whichever comes first.

(6) Records shall be maintained indicating time of receipt of alarm, name of guards responding, time dispatched to facility/area, time guards arrived, nature of alarm, and what followup actions were accomplished. Records shall be kept for a minimum of 1 year and shall be made available upon request to SSE inspectors during the conduct of scheduled and unscheduled inspections and surveys.

e. Equipment. All material, equipment, and sensors used in the IDS shall meet or exceed UL standards as evidenced by a UL listing mark on this specified material. Manufacturers of UL listed IDS equipment can be found in the UL Automotive, Burglary Protection, and Mechanical Equipment Directory. Copies of the directory may be obtained from: Underwriters Laboratories Inc., Publications Stock, 333 Pfingsten Road, Northbrook, IL 60062. Questions concerning approved types of alarm configurations shall be addressed to the SSE.

f. Installation. The IDS at the protected facility, area, or container shall be installed in accordance with UL standards by a UL listed alarm installer, or UL listed commercial central station. When connected to a commercial central station, the service provided shall be Grade AA (response time to an activated alarm shall not exceed 15 minutes and the connecting lines are electronically supervised to detect evidence of tampering or malfunction). In environments where Grade AA service cannot be provided, alternative installation and performance requirements shall be explored by the SSE and the facility manager, subject to the final approval of ACO-400.

825. AUTOMATED ACCESS CONTROL SYSTEMS. Automated access control systems which meet the criteria stated in this paragraph may be used to supplant employees or guards required for controlling admittance to CLOSED and RESTRICTED areas during working hours, with the prior approval of the SSE.

a. Manufacturers of automated access control equipment or devices must ensure in writing that their system will meet the following standards before the SSE may favorably consider such systems for protection of classified information.

(1) Gaining unauthorized access through normal operation of the equipment. The chances of an unauthorized individual gaining access through normal operation of the equipment are not greater than 1 in 10,000.

(2) Being rejected for authorized access through normal operation of the equipment. The chances of an authorized individual being rejected for access through normal operation of the equipment are not greater than 1 in 10,000.

b. The automated access control system must be capable of identifying the individual entering the area and authenticating that person's authority to enter the area.

c. Identification of individuals entering the area can be obtained by an identification (ID) badge or card or by personal identity.

(1) The ID badge or card must use embedded sensors, integrated circuits, magnetic stripes, or other means of encoding data that identify the facility and the individual to whom the card is issued.

(2) Personal identity verification identifies the individual requesting access by some unique personal characteristic, such as fingerprint, hand geometry, retina image, voice recognition, handwriting, or iris patterns.

d. In conjunction with an ID badge or card or personal identity verification, a personal identification number (PIN) is required. The PIN must be separately entered into the system by each individual using a keypad device. The PIN shall consist of four or more digits, randomly selected with no known or logical association with the individual. The PIN must be changed when it is believed that it has been compromised or subjected to compromise.

e. Authentication of the individual's authorization to enter the area must be accomplished within the system by comparing the inputs from the ID badge or card or the personal identity verification device and the keypad with an electronic data base of individuals authorized access into the area. A procedure shall be established for removal of the individual's authorization to enter the area upon reassignment, transfer or termination, or when the individual's personnel clearance is suspended, revoked, or downgraded to a level lower than required for area access.

f. Physical security protection shall be established and continuously maintained for all devices or equipment that constitute the system. The level of protection may vary depending upon the type of devices or equipment being protected with the basic intent of utilizing the security controls already in effect within the office or facility.

g. Access to records and information concerning encoded ID data and PIN's shall be restricted to individuals cleared at the same level as the highest classified information contained within the specific area or areas in which ID cards or PIN's are utilized.

826. ELECTRIC, MECHANICAL, OR ELECTROMECHANICAL DEVICES. Provided the classified material within the controlled area is no higher than SECRET, electronic, mechanical, or electromechanical devices which meet the criteria stated in this paragraph may, with the prior approval of the SSE, be used to supplant authorized employees or guards to control admittance to controlled areas during working hours. Devices may be used that operate either by push-button scramble combination which activates the locking device or by a control card used in conjunction with a push-button scramble combination, thereby excluding any system that operates solely by the use of a control card.

> NOTE: Push-button locks are susceptible to compromise by unauthorized persons viewing the lock as it is operated. To protect against this weakness, a scramble lock employs a random number sequence which electronically changes or scrambles the position of the numbers after each use. Other types of locks use a "spy-proof" cover or hood which blocks visual observation by anyone other than the person operating the lock.

827. DESIGNATION OF SECURITY CONTAINER CUSTODIAN. The office or facility manager responsible for the classified information shall designate in writing a custodian and one or more alternate custodians for each security container used to store classified information. The name(s) of the custodian and alternate custodian(s) shall be entered on an SF-700, Security Container Information, affixed to each container as described in paragraph 830a.

828. DUTIES OF THE SECURITY CONTAINER CUSTODIAN. The individuals designated as custodian and alternate custodians for the security container are responsible for ensuring that the security container is supervised, controlled, and operated in a manner that will ensure the safeguarding of its contents. Their duties include:

a. Ensuring that the container(s) is/are locked and checked at the end of each work day and when the container(s) is/are not under the continuous surveillance and physical control of an authorized person during the work day.

b. Confirming that classified material that has been withdrawn from the container has been returned to the container and that persons requesting or taking classified documents have the appropriate security clearance and need to know.

c. Ensuring that combinations to each security container are changed in accordance with the requirements of the latest edition of Order 1600.6 and this order.

d. Ensuring that classified documents removed from security containers are protected by cover sheets.

e. Conducting a careful search of the interior of a security container that is to be returned to storage to ensure that classified information or material has not been inadvertently left behind in the container. The search shall include all areas behind and under all drawers.

f. Ensuring that each security container has the correct documentation affixed to it to include SF-702, Security Container Check Sheet.

829. IDENTIFICATION OF SECURITY CONTAINERS. Each security storage container shall be assigned a number or symbol for identification. The identification shall be affixed by decal or placed in a conspicuous location on the upper right hand corner of the exterior surface of the first drawer of the container. The container identification shall not provide any information concerning the classification level of the container or the materials stored therein.

830. USE OF THE SECURITY CONTAINER INFORMATION SF-700. An SF-700 shall be prepared for each security storage container used for the storage of classified information.

a. Part 1. Part 1 of this form is unclassified and contains the name, address, and telephone number of those individuals who are to be contacted in the event the container is found open. Part 1 also contains the date the combination was last changed. Part 1 of the SF-700 shall be filled out and affixed to the right side of the interior of the locking drawer.

b. Parts 2 and 2A. Parts 2 and 2A of each completed SF-700 shall be marked with the highest classification that is authorized to be stored in the container. Parts 2 and 2A shall be stored by the SSE, or, as an alternative, shall be stored in a separate secure location approved by the SSE. A new SF-700 must be completed each time the combination is changed. One copy of the SF-700 shall be maintained by the SSE to ensure that combinations are changed on a timely basis.

831. USE OF THE SECURITY CONTAINER CHECK SHEET SF-702. An SF-702 shall be used on all security containers used for the storage of classified information.

a. Purpose. The SF-702 shall be properly filled out with the information concerning the identity of the container and its location affixed to the top or the side of the container in such a way as to be plainly visible. An appropriate entry shall be made on the SF-702 each time the security container is locked or unlocked.

b. Checked By Column. The "checked by" column on the SF-702 shall be used when the security container is secured at the end of the working day and when the container is to be left unattended. By initialing the "checked by" column, a person certifies that he or she has rotated the combination dial four times in both directions and has tried each drawer in the container to ensure that it is locked. Whenever possible, the "checked by" column of the SF-702 shall be initialed by a person other than the individual locking the container. When another individual is not available, the individual locking the container shall initial the "checked by" column.

832. CHANGE OF COMBINATIONS. Normally, combinations to security storage containers are changed by the custodian of the security container or by a cleared individual assigned that function within the FAA activity. Outside locksmiths shall not be used. If problems are encountered with changing the combinations, the SSE shall be contacted for assistance. When a combination is changed, the superseded combination is automatically declassified and may be destroyed without benefit of a destruction certificate. Combinations to security containers used for the storage of classified material shall be changed when one or more of the following conditions exist:

a. The security container is first received by the office or facility after it has been approved for the intended use by the SSE.

b. If it has been a year since the last time the combination was changed.

c. If there is reason to believe that an unauthorized person may have gained knowledge of the combination.

d. An individual has knowledge of the combination who no longer requires access to the container.

e. The container is designated for storage of material of a classification higher than the security clearance of individuals having knowledge of the current combination.

f. The SSE is required to comply with special requirements for safeguarding of NATO materials.

g. The container has been repaired and before it is placed back into service, and when the container is to be turned in to storage.

833. SAFEGUARDING COMBINATIONS TO SECURITY CONTAINERS. The combination to a security container used to store classified information shall be safeguarded at the same level required for the highest classification of information authorized to be stored in the container.

a. Combinations shall not be carried in wallets or on the person or be "hidden" in desks or other locations that are not approved for the storage of classified information.

b. Access to security container combinations shall be allowed only to persons having the appropriate security clearance, who are authorized access to the container, and who are determined to have a need to know.

834. STANDARD SUPPLY COMBINATION REQUIREMENTS. When a security storage container or high security padlock is to be removed from active service and returned to stock, a standard combination shall be set. The manager of the office or facility having responsibility for the security container shall notify the SSE a minimum of 30 working days in advance of the intent to turn-in the container. After the container has been completely emptied and searched to ensure that there are no remaining classified documents or materials, the manager shall ensure that the combination lock is set to 50-25-50 for the container. Combination padlocks shall be set to 10-20-30.

a. The individual responsible for the container shall ensure that a tag is prepared with the standard combination written on it together with the organizational symbol for the office returning the container or lock. The tag shall be affixed to a handle of the container or to the shackle of the padlock.

b. The standard combinations are reserved for cabinets and padlocks in storage and are prohibited for use in securing classified information.

835. ADMINISTRATIVE SAFEGUARD REQUIREMENTS FOR CLASSIFIED INFORMATION. Administrative controls are fundamental to maintaining proper safeguarding of, and managerial control and accountability for, classified information. The requirements listed in this paragraph are not all inclusive. It may be necessary to develop additional administrative procedures and controls for classified information depending upon the situation and the recommendations of the SSE. The SSE shall, during each survey and inspection of the office or facility, evaluate the effectiveness of the administrative and other controls in effect for the safeguarding of classified information. The SSE shall work closely with document custodians, managers, and other personnel to develop efficient and effective security procedures. The following mandatory requirements apply:

a. An activity or office which receives a classified document and has no secure storage capability shall immediately notify the SSE for guidance as to the appropriate action to be taken. Under no circumstances shall classified information be left unattended or in an unauthorized storage container.

b. Classified material shall not be displayed or left in an office when it is not under the direct visual surveillance and physical control of a cleared and authorized individual.

c. Cover sheets shall be used to protect classified documents from compromise. The cover sheet may be removed when the document is transmitted outside the office or facility or when it is placed in a file folder.

d. File folders containing classified information shall be marked top and bottom, front and back with the highest classification of material stored within the folder.

e. To preclude image transfer, front coated copy paper shall not be stored next to classified documents. Where it is necessary to store such material in the same container, it shall be separated from the classified printed matter by a sheet of nonsensitive paper. The same precautionary measures shall apply to plastic or other surfaces which come into contact with classified documents. When a transfer of information to the plastic or coated surface has taken place, the copy paper or plastic shall be safeguarded and destroyed as classified.

f. Offices maintaining classified material shall establish a system of checks to ensure that all classified information is properly secured at the end of the day or when the classified material is not under the continuous surveillance and physical control of an authorized, cleared individual.

g. Classified waste shall be segregated from unclassified material and safeguarded as classified material until it is destroyed. Individual users of classified material working in offices using "burn baskets" or other receptacles for classified waste are responsible for ensuring that all classified material placed in these receptacles is safeguarded from theft or compromise through the use of locking covers on the receptacles, or other safeguards. Receptacles of this type are not approved storage containers and they shall not be used under any conditions where they are not under the continuous physical control and visual observation of cleared and authorized personnel. Classified waste materials shall be protected from the time they are consigned to the classified waste until they are destroyed. Destruction shall be accomplished by authorized personnel using an approved destruction method.

h. Carbon paper, typewriter ribbons, and "one-time" typewriter ribbons used to process classified information shall be removed from the typewriter at the end of the day and safeguarded. Classified information shall not be read, studied, displayed, discussed, or used in any manner in any public location or conveyance (train, taxi, Metro, etc.).

i. Classified information shall not be discussed over nonsecure telephones or transmitted by any means other than prescribed in this order. Classified information shall not be removed from an office or facility except for official purposes and in accordance with the requirements of this order.

j. Persons hand-carrying classified material shall keep it in their personal possession at all times until it can be safeguarded in an approved container. Furthermore, the manager of the office or facility having responsibility for the information is responsible for ensuring that individuals designated to carry classified material are properly designated as couriers, and thoroughly briefed on their responsibilities for safeguarding the material, including the actions they are required to take in the event the classified material in their possession is lost, stolen, or otherwise subjected to actual or suspected compromise.

k. Classified material shall not be checked with baggage and shall not be left unattended by cleared personnel in automobiles, hotel rooms, aircraft, train compartments, buses, private residences, public lockers, etc.

l. Separate cassette type ribbons shall be utilized for typing classified information on typewriters and printers. These ribbons and cassettes shall be controlled and safeguarded in the same manner as the highest classification of information they have been used to process. They will be stored in an approved security container when not under the continuous surveillance and control of a cleared individual.

836. SAFEGUARDING CLASSIFIED MATERIAL DURING EMERGENCIES. In the event of a fire or other emergency (natural disaster, civil disturbance, etc.) requiring evacuation of office spaces, classified material shall be locked in approved storage containers. Persons away from their offices who are in possession of classified material shall ensure that such material is safeguarded. If it cannot be protected, it shall be destroyed beyond recognition with the prior concurrence or direction of the SSE or the manager who authorized the individual to carry the classified material.

837. EMERGENCY PLANS. In addition to the guidance which follows, refer also to the latest edition of Order 1600.6, which explains the requirements for FAA Occupant Emergency Plans. Each office and activity maintaining classified information shall coordinate with the SSE in the preparation of an emergency plan for the safeguarding and/or destruction of the classified material.

a. Approval of Plan. A copy of the written emergency plan shall be furnished to the SSE for approval.

b. Content. The plan shall include: the location, identity, and quantity of the classified information to be safeguarded or destroyed; a listing of the security containers and their identification numbers; names and contact identification for individuals who can authorize destruction; and the names and contact numbers of those personnel who are responsible for carrying out destruction procedures. The plan shall also list priorities for destruction and the training required for individuals responsible for destruction to include indoctrination in specific procedures to be followed. The plan should also cover any special destruction procedures that apply to such items as computer disks, film, etc.; location of destruction devices, equipment, and areas; and the location of all ancillary equipment required, such as carts, bags, hammers, burn bags, etc.

c. Relation to Contingency Plan. The classified document emergency destruction plan shall be coordinated with the facility contingency plan and the Facility Security Management Plan required by the latest edition of Order 1600.6.

838. RELOCATION OF CLASSIFIED STORAGE CONTAINERS. When it is necessary to relocate a classified information storage container physically, the manager of the

office or facility authorizing the relocation shall notify the SSE a minimum of 30 working days before the intended move. The SSE shall take appropriate action to inspect both the proposed new location and the security container to ensure that all applicable standards are met. Relocation of the classified storage container shall not be accomplished without the prior approval of the new site by the SSE.

839. CLASSIFIED CONFERENCES AND MEETINGS. Before planning or conducting a classified meeting, discussion, or presentation, FAA personnel shall coordinate with the SSE to ensure that all reasonable measures are taken at the proposed location to minimize the possibility of unauthorized visual, audio, or electronic surveillance which could compromise the data presented. Failure to coordinate with the SSE on matters involving classified presentations or meetings may result in a reportable security violation.

a. TOP SECRET. FAA conferences and meetings involving TOP SECRET information shall only be held in secure conference facilities that have been appropriately protected, inspected, cleared, and have a current certification for that level of classification by ACO-400, or another agency of the United States Government.

b. SECRET. FAA conferences and meetings involving SECRET information shall be coordinated with the SSE prior to the meeting. The SSE shall determine what precautionary measures are necessary to provide reasonable assurance that classified information will not be subject to compromise. Specific problems which arise concerning audio countermeasures shall be referred to ACO-400 for resolution. If the possibility of compromise is considered by the SSE to be unacceptably high, it is expected that classified information shall not be discussed at the meeting.

c. CONFIDENTIAL. Meetings, conferences, and seminars which involve presentation of CONFIDENTIAL information shall be coordinated with the SSE. The SSE shall advise the responsible FAA manager concerning area vulnerabilities or other concerns, and make appropriate recommendations for reducing the risk of compromise. If the possibility of compromise is considered by the SSE to be unacceptably high, it is expected that classified information shall not be discussed at the meeting.

840.-899. RESERVED.

CHAPTER 9. REPRODUCTION OF CLASSIFIED INFORMATION

900. REQUIREMENT. When it is operationally necessary to reproduce classified information, the number of copies shall be strictly limited to those required for official business. Restricting the reproduction of classified information decreases the risk of compromise and reduces the administrative burden of handling and safeguarding classified documents.

901. AUTHORIZATION TO REPRODUCE CLASSIFIED INFORMATION. The individual responsible for the classified information shall obtain authorization before reproducing the material. There are two types of authorization which shall be considered. In all cases, local authorization is required and, depending upon the classified information, the originator's authorization may also be required.

902. LOCAL AUTHORIZATION. The manager or supervisor responsible for the classified information shall ensure that local authorization is obtained in accordance with the following requirements:

a. Top Secret. For TOP SECRET information, the manager of the office that is requesting additional copies shall obtain prior local authorization to reproduce the information from the custodian of the SCP or, in the case of TOP SECRET, from the Top Secret Control Officer (TSCO). TOP SECRET material shall be reproduced only by the TSCO.

b. Secret and Confidential. For information classified SECRET and below, unless a notation on the document or its cover restricts reproduction, permission is authorized to reproduce the documents to the extent that is essential for efficient operations, and in accordance with the requirements of this directive and such additional implementing security guidance as may be required by the custodian of the SCP and/or the SSE.

903. ORIGINATOR'S AUTHORIZATION FOR REPRODUCTION OF TOP SECRET. The TSCO of the reproducing office shall obtain permission for reproduction of a TOP SECRET document unless otherwise marked from either the TSCO of the originating office or the TSCO of the operating element authorized to make initial distribution. Both the originating and reproducing offices shall maintain appropriate records to reflect the number of copies reproduced and observe all other requirements concerning the control and distribution of such copies.

904. ACCOUNTING FOR REPRODUCED COPIES OF CLASSIFIED INFORMATION. FAA offices and activities that reproduce paper copies of classified documents shall maintain records to show the number and distribution of reproduced copies:

a. Of all TOP SECRET documents.

b. Of all documents covered by special access programs distributed outside the originating agency.

c. Of all documents distributed within the office or activity if required by the special access program; and

d. Of all SECRET and all CONFIDENTIAL documents which are marked with special dissemination and reproduction limitations.

e. All reproduced copies shall specify the authority for reproduction and the number of copies made.

905. MARKING REPRODUCED CLASSIFIED INFORMATION. The supervisor or manager is responsible for ensuring that all reproductions of classified material are conspicuously marked with the same classification markings and any special warning notices as the material being reproduced. Copies of classified material shall be reviewed after the reproduction process to ensure these markings are visible.

906. REPRODUCTION EQUIPMENT AND AREAS. Reproduction equipment and areas can normally be categorized in terms of office copiers and the areas in which they are located, and printing and photographic processes and the areas in which these activities are located.

907. CONTROL OF OFFICE COPIERS. Reproduction of classified material shall be accomplished only on machines that are under the continuous control of cleared U.S. personnel. An office copy machine shall be specifically approved in writing by the SSE for use in the reproduction of classified information. This approval shall specify the model and serial number of each item of reproduction equipment being approved together with the physical and technical security safeguards that must be followed when using the equipment. The manager of the office or facility responsible for the classified material shall implement the safeguarding procedures prescribed by the SSE before the equipment is used to reproduce classified material.

a. Location. The manager of the office or facility having responsibility for the safeguarding of classified material shall ensure that office copiers approved for the reproduction of classified information are physically located in areas where safeguards against unauthorized physical and visual access are in effect.

b. Standard Operating Procedures (SOP). Specific guidance shall be prepared in the form of SOP's for each type of office copier in the facility that is to be used for the reproduction of classified information. The SOP shall be coordinated with the SSE and shall identify specific security hazards associated with each type of equipment. The SOP shall also indicate the correct practices to be followed when reproducing

classified information to include the procedures that must be followed for obtaining reproduction approval and authorization.

c. Signs. Copiers that are approved for reproduction of classified information shall be identified by appropriate signs posted in a conspicuous location in proximity to each copier. The wording on the signs shall identify the copier as "Approved for the Reproduction of Classified." The sign shall indicate in smaller letters who the approval authority is and how that individual may be contacted.

(1) The signs should use block letters against a high contrast background and should be sufficiently large so that they are easily legible at a distance of 20 feet.

(2) FAA Form 1600.49, No Classified Reproduction Authorized, shall be conspicuously posted near reproduction equipment that is not authorized for use in reproducing classified information.

908. PROHIBITIONS. In order to minimize the possibility of loss or compromise of classified information in the reproduction process, individuals responsible for the reproduction of information shall not:

a. Leave flatbed reproduction equipment with classified documents remaining under the cover.

b. Leave reproduction equipment before the last copy of classified material has emerged from the delivery slot.

c. After completing a classified run, omit the precaution of running three or four sheets of blank paper through the copy machine to ensure that there is no residual image produced.

d. Reproduce classified information under circumstances which could permit unauthorized persons to observe visually or acquire physically the classified information.

e. Leave the reproduction equipment before ensuring that all classified material is accounted for when the equipment has failed to deliver the number of copies mechanically ordered.

f. Leave before clearing all damaged copies from inside the equipment or leave the reproduction equipment unattended when processing classified material and there is an equipment malfunction.

g. Dispose of classified material or classified waste using procedures that have not been approved by the SSE and are not in compliance with this order.

h. Fail to destroy classified pages or classified waste properly in accordance with this order.

i. Fail to destroy classified negatives or materials when using diffusion transfer or dry transfer machines.

j. Fail to safeguard against a front-coated copy page transferring an image to the carrier held inside certain single copy duplication machines or against producing a "ghost" image on the next reproduced copy if a screen carrier is used.

k. Fail to run blank pages through a copier or printer toner cartridge prior to disposing of the cartridge.

l. Fail to use only Type 1 (back coated) thermal copy paper when reproduction is done by the thermal copy process.

m. Fail to handle as classified waste; therefore, personnel shall use slip sheets which are placed between the film sheets in the diazo process.

909. CONTROL OF PRINTING AND PHOTOGRAPHIC AREAS AND PROCESSES. Pressrooms, darkrooms, composition, bindery, and proofreading rooms (or appropriate portions thereof) shall be designated as "Closed Areas" when a classified production is in process. Admittance to the area shall be limited to persons who have the requisite security clearance and whose presence is necessary.

910. PRODUCTION CONTROL RECORDS. While the production control records remain with the classified job to which they relate, they shall be plainly and conspicuously marked or stamped at the top and bottom with the same classification markings as the material being reproduced. Production control records shall be marked with a notation indicating that they are unclassified when separated from the classified material being produced unless they contain classified information.

911. PRODUCTION AREA CONTROLS. During the layout, composition, platemaking, presswork, and bindery stages of the reproduction of classified material, controls shall be established to deny unauthorized personnel access to the immediate area in which such work is being performed. If the material cannot be adequately safeguarded by storage in an approved container or by supervision of an appropriately cleared employee, a controlled area shall be established in accordance with the provisions of chapter 8 of this order.

912. PRESSROOMS AND BINDERY AREAS. While the press is being made ready or being run, the press itself shall be identified and marked with the same classification as the classified information being run. The press shall remain so identified until the

run has been completed and all classified material removed. Marking and identification are not required for press runs of short duration, provided the run is completed prior to the end of the workday. Plates, blankets, chases, and the like need not be removed from the press at the close of working hours when the press run is incomplete, provided the area meets the requirements of this order for a Closed Area during nonworking hours specified in chapter 8.

913. COMPOSITION AREA. Linecasting (for example, intertype and linotype) and photocomposition machines shall be identified and marked the same as the classified information being set in type, except for the jobs of short duration completed prior to the end of the working day. Slugs (that is, lines cast on a linecasting machine), coded tapes, ribbons, negatives, and so on need not be removed from the machines at the close of the workday when the composition is not completed, provided the area meets the requirements for a Closed Area during nonworking hours specified in chapter 8.

914. DARKROOMS. Admittance to all film processing units shall be restricted to cleared employees who are assigned to the particular job or jobs involving classified information.

915. PROOFREADING AREAS. Proofreading areas shall be controlled by physical barriers capable of preventing visual or audio access and entrance by unauthorized persons.

916. SHIPPING ENTRANCES. Shipping entrances shall be secured when classified information is in the area. Loading and unloading operations shall be performed under the supervision of a cleared employee.

917. SPECIAL CONDITIONS.

a. Overruns. All assembled copies of printed material not spoiled during a printing operation, which are in excess of the number of copies ordered, shall be designated as overruns. Overruns shall be held to a minimum. An exact count of the overruns shall be maintained and they shall be entered into the accountability system or promptly destroyed by an approved method.

b. Proofs. A record shall be kept of the number and disposition of proofs. Galley or page proofs approved by the requestor shall be retained until the product is delivered, and shall be returned to the customer along with the original manuscripts.

c. Waste Disposal. Properly identified waste containers shall be provided at each production point at which waste spoilage, trimmings, or cuttings accumulate. Waste shall include paper stock used for press make-ready, spoilage during running, printed copies spoiled during bindery make-ready, or excess copies of individual pages that are not to be assembled to form a completed product.

d. All material used in production that contains classified information, e.g., negative flats, layouts, masters, drums, vellums, type, plates, will be properly safeguarded and either destroyed as classified waste or entered into the accountability system and safeguarded and controlled in accordance with the provisions of this order.

e. All material shall be properly safeguarded in accordance with the requirements of this order for classified information of the same classification level. Plates and rubber blankets used on a classified production may be reused only on other classified jobs. Between runs they will be stored in approved security containers and will be marked to indicate the highest category of classified information they were used to process.

f. Materials used in Production.

(1) All materials used in production, which contain classified information (that is, negative flats, layouts, masters, dummies, vellums, stencils, composition tapes, proofs, tympan sheets, negatives, types, plates, and so on), shall be safeguarded as required by chapter 8 for the level of classified information involved and, immediately after completion of the work, destroyed by approved methods or returned to the requestor along with the finished job.

(2) Rubber blankets used in classified production may be retained for reuse in classified and unclassified production provided they are washed to remove any classified information, are marked with the highest classification of any information for which the blanket has been used, are entered into the accountability system, and are safeguarded according to the appropriate classification level. When no longer serviceable, or reuse is not desired, the rubber blanket shall be destroyed by approved methods for the level of classified information involved.

(3) Plates used on a classified production shall not be reused, and shall be destroyed by approved methods. Regraining plates shall not be considered as an authorized method of destruction.

918. INSPECTION REQUIREMENTS. The manager of the SSE shall ensure that classified document reproduction procedures are evaluated during each scheduled and nonscheduled inspection and survey of the office or facility.

919.-999. RESERVED.

CHAPTER 10. PACKAGING CLASSIFIED INFORMATION

1000. GENERAL. The term "classified information transmission," as it is used in this order refers to the means used to transfer national security classified information from one location to another location. This transfer process may involve the physical relocation of a document or it may refer to the electronic transmission of the information content. In either case, the person responsible for the classified material is also responsible for ensuring that the material is packaged and/or transmitted in a manner that is approved for the classification level concerned.

1001. PACKAGING REQUIREMENTS FOR CLASSIFIED INFORMATION. The individual who possesses the classified information is responsible for ensuring that it is packaged and prepared in accordance with this order. The following paragraphs provide specific guidance for packaging classified information. Questions concerning packaging that are not covered in the section should be referred to the SSE.

a. Wrapping. Classified material shall be double wrapped or packaged in opaque inner and outer sealed envelopes, wrappings, or cartons. Packaging material, whether it consists of envelopes or containers, shall be of such strength and durability that it will provide security protection during transit and will prevent items from breaking out of the containers or envelopes. The use of sturdy packaging material and strong sealing tape also provides an additional measure of protection against undetected tampering with the envelope or container. Bulky packages and large envelopes shall be sealed with kraft tape, laminated with asphalt, and containing rayon fibers or nylon sensitive tape or equivalent.

b. Security Control Point (SCP). In offices and facilities where there is an SCP, the manager responsible for the classified material shall ensure that it is taken to the SCP and packaged by, or under the supervision of, the custodian of the SCP or alternate. When there is no SCP, the manager shall ensure that the classified material is taken to the classified information account custodian (CIAC) or the alternate classified information account custodian (ACIAC) and packaged under their supervision.

c. Overseas Locations. In overseas locations, if a question arises concerning packaging of classified material for transmission and it is not possible to contact the SSE, the manager or employee responsible for the classified material shall contact the nearest Department of State (DOS) Regional Security Officer (RSO) for assistance.

d. Inspection. Classified information that has been packaged for transmission shall be given a final inspection prior to transmission to ensure that it has been properly packaged. This inspection shall be accomplished by the custodian of the SCP, if available, or by the CIAC or the ACIAC. If none of these individuals is available, the employee preparing the package shall conduct the inspection.

1002. REQUIREMENTS FOR PREPARING CLASSIFIED PACKAGES. When assembling a classified package, the inner envelope or wrapper shall be of sturdy material and shall be marked at the top and bottom and, in the case of boxes, on all sides, with the highest classification of the material contained therein. Warning notices and special handling instructions will also be affixed to the inner wrapper. The outer envelope or wrapper shall also be of sturdy material. Markings affixed to the outer wrapper shall not indicate the classification level or that classified information is enclosed. Markings on the inner wrapper shall not be visible through the outer wrapper. The outer wrapper or envelope shall be addressed to an official Government office or cleared contractor facility and not to a specific individual. The inner wrapper only may be marked with an "attention line" with the routing symbol or organizational component of the addressee. The outer and inner envelope or wrapper shall contain the complete organizational return address of the individual preparing the package.

1003. RECEIPT REQUIREMENTS AND TRACER ACTION. A receipt shall be prepared whenever TOP SECRET or SECRET material is transmitted. For CONFIDENTIAL material a receipt is optional. The receipt shall be attached to or enclosed with the inner envelope or wrapper and shall identify the sender, the sender's and the recipient's addresses, and the unclassified description of the material transmitted. The receipt shall not contain classified information. The receiving office or activity should verify the contents of the envelope or package, sign the attached receipt, and promptly return the signed receipt to the sender. Tracer action shall be initiated by the FAA office transmitting the classified material if the signed receipt has not been returned within 30 working days indicating that delivery has been made. Indications that the package containing the classified material has been lost or misplaced shall be reported immediately to the manager having responsibility for the classified material who shall in turn notify the SSE.

1004. PACKAGING REQUIREMENTS FOR NONMAILABLE BULK CLASSIFIED MATERIAL. Classified material that falls into this category is not likely to be encountered on other than rare occasions by FAA personnel. However, should the occasion arise when it is necessary to prepare a package of classified material that is too bulky for mailing, the requirements of this paragraph shall apply. For special shipping requirements involving classified material, the office or activity manager responsible for the classified shipment shall coordinate closely with the SSE in making shipping arrangements and, prior to actual shipment, ensure that the safeguards provided are adequate. In overseas areas, if the SSE is not accessible, the FAA manager responsible for the material to be shipped shall coordinate with the DOS, RSO to determine the appropriate packaging and shipping requirements for the classified material.

a. Packaging when the Internal Component is Classified. If the classified material is an internal component of an item of equipment that can be packaged and the outside shell or body is not classified, and if the outside body or shell completely shields the

classified component, then the shell or body of the item may be considered as the inner wrapper. This configuration still requires an appropriate outer wrapper be provided.

b. Packaging when the Internal Component is Classified and Inaccessible. If the classified material is an inaccessible internal component of a bulky item and cannot be packaged with reasonable effort, the outside shell or body may be considered as the outer covering or wrapper provided the outside shell is not itself classified. If the outside shell or body is classified, the item shall be draped with an opaque covering of canvas or other sturdy material. The covering shall be secured to prevent inadvertent exposure. Packaging of this type must be approved by the SSE prior to shipment.

c. Specialized Containers. Specialized shipping containers including closed cargo transporters, may be used as the outer wrapping or cover subject to the prior approval of the SSE.

d. Marking. When marking bulky nonmailable packages, the classification, address of the intended recipient, and the complete organizational return address of the transmitting office shall be marked on the inner wrapper. The outer wrapper shall have the organizational address of the recipient and the complete organizational address of the sender. The outer wrapper shall not have any marking that would indicate that the contents are classified.

1005.-1099. RESERVED.

CHAPTER 11. TRANSMISSION OF CLASSIFIED INFORMATION

1100. REQUIREMENT. Under no circumstances will United States classified information be transmitted by other than the approved methods described in this order. The same applies to information relating to foreign government classified material for which the FAA has an actual or implied obligation to provide protection.

1101. TRANSMISSION OF TOP SECRET INFORMATION. TOP SECRET material shall not be mailed. When it is necessary to transmit TOP SECRET material, the Top Secret Control Officer (TSCO) is responsible for ensuring that the methods and procedures used comply with the requirements of this order. Questions concerning the transmission of TOP SECRET information which are not covered in this order shall be referred through the TSCO to the SSE. TOP SECRET information may be transmitted by one or more of the following procedures when specifically approved by the TSCO:

a. Oral discussion in person between properly cleared individuals who are authorized access to the information with care taken to ensure that the discussion cannot be overheard or lip movements visually observed by unauthorized persons.

b. Personnel authorized access to the information and specifically cleared, designated, and approved by the TSCO as couriers for TOP SECRET. When a requirement exists to hand-carry TOP SECRET material, the manager who is responsible for the material shall, in coordination with the TSCO, ensure that two FAA personnel cleared for TOP SECRET accompany the material at all times during its transmission. Normal mail and messenger service of an activity shall not be used. Postal service and delivery services shall not be used.

c. TOP SECRET material may be transmitted by couriers of the Defense Courier Service (DCS) and by Accompanied State Department Diplomatic Pouch.

d. Electronic transmission of TOP SECRET information shall be accomplished using equipment, methods, and procedures that have been specifically approved for the purpose by the National Security Agency (NSA).

1102. TRANSMISSION OF SECRET INFORMATION. SECRET information shall be transmitted by any method approved for the transmission of TOP SECRET. Limitations may be imposed on the use of DCS for other than TOP SECRET. The custodian of the SCP and the CIAC are responsible for ensuring that correct transmission procedures are utilized for SECRET material. In addition to the DCS, SECRET material may be transmitted by the following methods:

a. FAA personnel possessing a current SECRET or higher clearance who have been

formally designated as couriers and have been briefed by the SSE or an authorized representative of the SSE regarding their responsibilities as couriers or escorts, and who otherwise comply with the requirements of this order concerning couriers.

b. U.S. Postal Service registered mail within and among the 50 states, the District of Columbia, and Puerto Rico, provided the material does not pass out of the control of U.S. citizens. The prior approval of the SSE shall be obtained for transmission of SECRET material by this method outside the contiguous 48 states and the District of Columbia.

c. U.S. Postal Service Express Mail Service within and among the 50 States, the District of Columbia, and Puerto Rico, provided the material does not pass out of the control of U.S. citizens. Express mail service may be used only if mission essential within established cost and accountability restrictions. U.S. Postal Service Express Mail Label 11-B shall not be executed under any circumstances. Shipments shall be processed through mail distribution centers or delivered directly to a U.S. Postal Service facility or representative. The use of external or street-side express mail collection boxes is prohibited. Prior coordination with the SSE shall be accomplished before utilizing express mail services for the transmission of SECRET information.

d. For transmission of documents that are being sent to a Canadian Government office or facility, the use of U.S. or Canadian registered mail is acceptable with the prior approval of the SSE. The FAA office transmitting SECRET material shall obtain a registered mail receipt and shall request a return receipt as confirmation of delivery.

e. U.S. Postal Service registered mail through Army, Navy, or Air Force Postal Service facilities outside the United States and its territories provided that the U.S. postal facility to which SECRET material is to be sent has the capability to receive registered mail. If the postal facility does not have the capability to receive registered mail, it is not approved for use by FAA personnel in transmission of SECRET or CONFIDENTIAL information.

f. Qualified, cleared carriers are authorized to transport SECRET material via a Protective Security Service (PSS) under the Department of Defense Industrial Security Program. This may be used only within the United States when the size, bulk, weight, and nature of the shipment make other methods impractical.

g. U.S. Government carriers under escort of cleared personnel. This includes Government vehicles, aircraft, ships of the United States Navy, or civil service manned U.S. ships. Cleared operators, officers of ships, or pilots of aircraft who are U.S. citizens may be designated as escorts if control and surveillance of the carrier is maintained 24 hours a day. The escort shall protect the shipment at all times, through personal observation, placing the shipment in protected storage, or other measures designed to prevent inspection, tampering, pilferage, or unauthorized access until

delivery. Observation is not required while the shipment is stored in an aircraft or ship in connection with flight or sea transmittal provided the shipment is in a compartment that is not accessible to unauthorized persons or is loaded in specialized shipping containers, including closed cargo containers. The container or compartment must be sealed in such a way that unauthorized access is not possible without detection. Guidance for this type of shipping procedure shall be obtained from the SSE prior to shipment.

1103. TRANSMISSION OF CLASSIFIED MATERIAL VIA THE DEPARTMENT OF STATE ACCOMPANIED DIPLOMATIC POUCH SYSTEM (DOS/ADPS). When it is necessary to transfer classified material outside the continental United States, FAA personnel shall use either secure telecommunications, approved Armed Forces Postal Service facilities, or the DOS Accompanied Diplomatic Pouch System (DOS/ADPS). For example: In a situation where it might be necessary to send a classified document from FAA offices in Brussels, Belgium, to FAA or other authorized recipient offices in Frankfurt, Germany, the transmission could be accomplished by DOS/ADPS. Similarly, if it is desired to send a classified document from FAA headquarters, Washington, DC, to FAA Brussels, the transmission could also be accomplished by DOS/ADPS. In order for classified material to be sent from the United States to an overseas destination using the DOS/ADPS, it is necessary for the office or element desiring to transmit the classified material to establish prior coordination with the DOS through ACO-400, Washington, DC, to ensure that the procedures to be followed are understood. Within the United States, classified material to be shipped via the DOS/ADPS may be transmitted to the DOS by mail or by courier.

a. To send classified material to the DOS by mail, the FAA office preparing the classified material shall ensure that the package has been prepared in accordance with the requirements of this order and that it is shipped to DOS via registered mail. The outer envelope or wrapper shall not reflect the final destination of the material but shall be addressed to: Chief, Classified Pouch and Mail Branch, Department of State, Washington, DC, 20520-0528. The DOS Pouch Room will open the outer envelope or wrapper and place the inner envelope or wrapper and its contents in the classified pouch and forward to the appropriate overseas post. The inner envelope shall contain the address including the specific post. It will be marked on both sides with the highest classification of the material to be transmitted. The inner envelope shall have a registration form, preferably DOS Optional Form 120, "Diplomatic Pouch Mail Registration." If this form is not used, the DOS Pouch Room will utilize the 9-digit U.S. Postal Service Registered Number.

b. Classified mail can also be hand-carried to the DOS for inclusion in the Diplomatic Pouch. When this procedure is used, the classified material shall be packaged and addressed in accordance with the requirements of this order, and shall

be delivered by a cleared FAA courier to the Classified Pouch and Mail Branch, Department of State, Washington, DC. The package will be receipted for by a representative of the Pouch and Mail Branch. The courier shall return the signed copy of the receipt to the appropriate FAA SCP.

1104. RETURNING CLASSIFIED MATERIAL FROM OVERSEAS LOCATIONS. FAA offices overseas desiring to send classified material back to the United States shall use secure telecommunications, approved Armed Forces Postal facilities, or DOS/ADPS. When using the DOS/ADPS packaging requirements, this order shall be followed with certain exceptions. The classified material shall be double wrapped as prescribed. The double wrapped envelope shall then be inserted into another envelope so that the outer wrapper of the double wrapped envelope now becomes the inner wrapper of the package to be delivered to the DOS. In this arrangement, the inner envelope has no classification markings but is completely addressed with the address of the recipient and the sender. The outer envelope will contain classification markings and the mailing address as well as the complete return address of the sender. The material shall be delivered to the U.S. Embassy Communications Officer who will insert the package into the diplomatic pouch. The DOS/RSO can be of assistance in making arrangements for the use of the DOS/ADPS and should be consulted. When the pouch arrives at the Main State Department Pouch Room in Washington, DC, the DOS will prepare an outer envelope, place the package inside, and will mail the package, via registered mail, to the address indicated on the inner envelope.

1105. TRANSMISSION OF SECRET AND CONFIDENTIAL MATERIAL WITHIN AN ACTIVITY OR OFFICE. If it is required to transmit SECRET or CONFIDENTIAL material from one building to another which requires travel on a public street or road, the material shall be packaged in accordance with the requirements of this order except that a locked briefcase may be used as the outer wrapper. For hand-carrying within the same building, a cover sheet shall be affixed to the document to prevent unauthorized disclosure.

a. If an activity's mail and messenger system is used to deliver SECRET and CONFIDENTIAL material, the material shall be placed in a single opaque, sealed envelope with the classification marked on the envelope. Only messengers cleared for access to the highest level of classification being transmitted shall be allowed to deliver the material.

b. When an office with classified material physically moves within a building, or from one building to another, the material shall stay in the locked security container or be securely packaged for the move. The CIAC, ACIAC, or other cleared individual shall accompany the container with the material at all times while it is in transit. The

manager of the office or activity responsible for the classified material shall ensure that the SSE is notified a minimum of 30 working days prior to relocating classified material or moving a security container containing classified material.

1106. TRANSMISSION OF BULK CLASSIFIED MATERIAL. To ensure that classified material is properly received and protected upon delivery, the activity responsible for shipping bulk classified material by Government or commercial carrier shall notify the consignee (including a military transshipping activity) in advance of the date of arrival of the nature of the shipment, anticipated time and date of delivery, means of shipment, and number of seals if used. The consignee shall also be requested to notify the consignor of any shipment that has not been received within 2 working days of the estimated time of arrival. Upon receipt of such a notice, the consignor shall immediately request the carrier to trace the shipment. The office responsible for shipping the material shall annotate the bills of lading to require the carrier to notify the consignor immediately if the shipment is delayed en route. Bills of lading or other shipping documents shall not indicate that the shipment is classified. Bulk material weighing less than 200 pounds shall be shipped only in a closed vehicle.

1107. TRANSMISSION OF CLASSIFIED INFORMATION BY SECURE TELECOMMUNICATIONS. Electrical transmission of classified information to points within or outside an FAA activity shall be accomplished only when approved by ACS-1 using NSA-approved telecommunications equipments and procedures. Requirements for support involving the use of secure telecommunications shall be coordinated in advance with the SSE.

1108. TRANSMITTING CLASSIFIED INFORMATION IN SUPPORT OF OFFICIAL VISITS. If it is necessary for operational purposes for an FAA employee to have SECRET or CONFIDENTIAL material during an official visit to a facility in the continental United States, and the facility being visited does not hold the material, the classified material may be forwarded subject to the requirements of this paragraph. The manager or supervisor authorizing the visit is responsible for approving the request for the classified information. In so doing, the manager shall ensure that he/she has coordinated with the custodian of the SCP or the CIAC and determined that the employee has the appropriate clearance for the material being requested and has an official need to know. The manager authorizing the transfer of the information shall ensure that the material is marked, packaged, and controlled in accordance with this order. The material shall be double wrapped and the inner envelope, in addition to the required classification and address markings, shall be marked "Hold for the Arrival of (Name of employee requesting the material)." Finally, the manager shall ensure prior to having the material forwarded that the receiving facility is capable of meeting all of the safeguarding and clearance requirements of this order.

1109. TRANSMISSION BY COURIER. Under extreme circumstances, if the visit and the need for the material was not anticipated in time to forward the material, the manager who is responsible for the classified material may approve SECRET or CONFIDENTIAL material being hand-carried by an appropriately cleared FAA employee designated as a courier. The manager is responsible for ensuring that the employee meets all of the requirements of this order pertaining to courier selection, briefing, etc. If a courier is utilized, only those portions of a classified document essential for the visit shall be taken. In the case of a SECRET document, any sheets removed from the document shall be accounted for and controlled by the SCP. If the facility or office does not have an SCP, guidance shall be requested from the SSE. The following additional requirements apply:

a. An itemized list of the classified material shall be prepared. A copy of this list shall be retained by the SCP and by the manager approving the courier delivery. If the facility or office does not have an SCP, the manager shall retain a copy and the second copy shall be retained by the CIAC. The employee designated as courier shall retain a copy.

b. A Classified Material Cover Sheet shall be attached to the material. The material shall then be double wrapped and sealed in opaque envelopes or wrapping and fully addressed as prescribed by this order.

c. The individual designated as courier shall be required to read and understand the provisions of this chapter and shall be formally briefed by the manager or by the CIAC on his/her responsibilities for the safeguarding of the classified material. See appendix 8 for the courier briefing format and content.

d. The individual designated as a courier shall be provided with a courier letter using the format contained in appendix 9. The courier letter shall be signed by the office or facility manager.

1110. RETURN OF CLASSIFIED INFORMATION UPON COMPLETION OF OFFICIAL VISIT. When the official visit for which classified information has been provided is completed, the FAA employee responsible for the classified information shall make arrangements with the SCP or the CIAC at the facility to repackage the material for return to the office or facility from which it was sent. All classified material shall be receipted for by the SCP or the CIAC at the time that it is accepted from an FAA employee. The properly packaged classified material shall be returned using one of the approved transmission methods described in this order.

1111. TRANSMISSION OF CLASSIFIED INFORMATION BY FAA EMPLOYEES. FAA employees are not authorized to carry or possess classified information or material outside Government facilities or Government approved contractor facilities unless they

are officially designated as couriers. Requirements for courier designation are listed in appendices 7 and 8. The courier, when designated, shall be issued a courier letter as shown in appendix 7 and shall produce this letter to show to authorized persons when necessary. The employee shall also be thoroughly familiar with the contents of this order and the courier instructions in appendix 8.

1112. COURIER TRAVEL WITHIN THE CONTIGUOUS 48 STATES AND OVERSEAS. Within the contiguous 48 States, presentation of the required courier authorization letter together with official travel orders should permit the employee to travel by air or other modes of transportation without having to subject the classified material to inspection at airport screening operations and other official screening points. It is always a sound idea, however, to coordinate ahead of time with the SSE and advise them of the courier's itinerary so that they may, if necessary, arrange for the local Civil Aviation Security Field Office (CASFO) to coordinate with the airport authorities to facilitate passage through screening points. Any difficulty encountered should be reported to the appropriate manager and the SSE. FAA employees are not authorized to carry classified material in overseas areas outside U.S. Government control without the express approval of ACS-1.

1113. TRANSPORTING CLASSIFIED INFORMATION BY COURIER ABOARD COMMERCIAL PASSENGER AIRCRAFT. Hand-carrying classified information aboard commercial aircraft is discouraged. In the event that an urgent operational need exists, the manager responsible for the classified material shall coordinate with, and receive the prior approval of, the SSE before authorizing the carriage of any classified information or material aboard a commercial passenger aircraft. Classified information and material will not be checked in luggage, transported in baggage compartments, or otherwise handled by any means that separates the courier and the classified information. The FAA courier shall possess an appropriate DOT/FAA picture identification card or credential and a current, signed courier letter.

1114. SCREENING OF CLASSIFIED MATERIAL BEING TRANSPORTED BY COURIER. If the classified information is contained in envelopes, it shall be double wrapped in accordance with the requirements of this order and shall have no metal bindings. The envelopes shall be offered for x-ray screening. The screening official is not authorized to open the envelopes or read the classified material in the custody of an officially designated courier. However, the screening official may check the envelope by x-ray, flurrying, feel, weight, etc., without opening the envelope itself. A briefcase shall not be used as an outer wrapper.

1115.-1199. RESERVED.

CHAPTER 12. DESTRUCTION AND DISPOSAL OF CLASSIFIED INFORMATION

1200. REQUIREMENT. When classified material is no longer needed, it shall be disposed of in an authorized manner or destroyed by an approved destruction method. When classified material that is no longer needed continues to be maintained, it increases the cost of storage and also increases the danger of possible compromise. The latest edition of Order 1350.15, Records Organization, Transfer, and Destruction Standards, specifies what material classified or unclassified shall be permanently retained and forwarded to a records repository. It is the responsibility of the manager of the office disposing of classified information to determine specific eligibility for disposition or destruction from a records management standpoint. Questions concerning this process should be directed to the SSE. Nonrecord copies of classified documents may be forwarded to the SCP for authorized destruction at any time. Classified material forwarded to a records repository shall be reviewed for regrading and shall be accounted for, packaged, and transmitted in accordance with the requirements of this order.

1201. PREPARING CLASSIFIED MATERIAL FOR DESTRUCTION. Classified documents shall be forwarded to the SCP or, in the case of TOP SECRET, to the Top Secret Control Officer (TSCO) for destruction. DOT Form 1600.22, Destruction of Classified Record, or DOT Form 1600.29, Classified Material Receipt, shall be completed when destroying TOP SECRET and SECRET documents. FAA Form 1600-35, Classified Document Register, shall be annotated to indicate the destruction of all TOP SECRET and SECRET material. The SCP shall destroy or arrange for destruction of documents classified SECRET and below. Destruction of TOP SECRET documents shall be supervised by the TSCO. Documents shall not be torn or mutilated before forwarding to the SCP or the TSCO.

1202. CLASSIFIED WASTE. TOP SECRET waste materials shall be sealed in an envelope and turned in to the TSCO for destruction. Classified communications security (COMSEC) material shall be returned to the COMSEC manager for destruction. All SECRET and CONFIDENTIAL classified waste materials such as carbon sheets, typewriter ribbons, plates, stencils, masters, stenographic and handwritten notes, and draft material, that do not have a control number assigned by the SCP shall be sealed in an envelope or in a "burn bag" for classified material and forwarded promptly to the SCP for destruction. Waste material does not need to be itemized. The envelope or bag shall be marked "CLASSIFIED WASTE," and the material shall be safeguarded and stored in the same manner as prescribed for classified information of the same level. If the classified waste is material other than documents, such as computer disks, photographs, printer cartridges, etc., the SSE shall be contacted through the SCP or the TSCO as appropriate to determine the approved destruction procedure.

1203. DESTRUCTION METHODS. The object of any destruction method for classified material is to destroy the material so completely that recovery of classified information from the residue will be impossible. Equipment and procedures used for destroying classified materials shall be approved for that purpose by the General Services Administration (GSA) and/or the National Security Agency (NSA) and also be approved by the SSE. All requests for acquisition of destruction equipment must be coordinated with, processed through, and approved by the SSE.

a. Burning is an approved method of destruction provided the container has been approved by the SSE and the ashes are sifted after burning to ensure that no fragments of the documents remain. Burning has some adverse environmental impacts and for this reason is generally less desirable for routine destruction of classified than other approved techniques.

b. Pulping, pulverizing, chopping or shredding, are approved methods for destruction of classified material provided the equipment is of a type and model that has been specifically approved by the GSA or NSA for the destruction of the type of classified material concerned. Assistance as to the type, size, style, and approved equipment can be obtained from the SSE. The SSE shall be consulted prior to procurement of such equipment. Documents destroyed in this manner shall be reduced to fragments that are no larger than 5 millimeters (0.2 inches) in any dimension. These types of equipment generally employ cutting blades and filter screens which wear with use and should be checked at least every 6 months to ensure that they are in good working condition.

c. Melting, chemical decomposition, and mutilation are destruction methods employed for classified material other than documents. Because of the potential hazards posed to employees and to the environment by the use of these techniques, any office considering their use shall coordinate with ACO-400 through the SSE prior to using any of these methods for destruction of classified material.

1204. DESTRUCTION RECORDS. TOP SECRET and SECRET destruction shall be accomplished in the presence of a witness. A destruction certificate is required for TOP SECRET and SECRET to include the identification and description of the document/material destroyed, control number, and signatures of the destruction official and the witness. DOT Form 1600.4, Classified Material Record, is authorized for and used as a destruction certificate provided it has all of the required information. Destruction certificates shall be maintained at the security control point (SCP) and Document Control Station (DCS) for at least 4 years. Any other accountability records at the SCP and DCS, including the DOT F 1600-35, shall be annotated to reflect the destruction. A destruction certificate is not required for CONFIDENTIAL material.

1205.-1299. RESERVED.

CHAPTER 13. INTERNATIONAL SECURITY REQUIREMENTS

1300. GENERAL. This chapter contains information on the United States National Disclosure Policy, U.S. laws and regulations, and bilateral security agreements, which are executed between the U.S. Government and certain friendly and allied foreign governments, governing the exchange and protection of classified information.

1301. POLICY. An appropriate U.S. Government disclosure authority shall determine whether (1) classified information is releasable to a foreign government, (2) the disclosure is in compliance with U.S. National Disclosure Policy, laws, and regulations, and (3) the information can be adequately protected by the foreign recipient. These decisions to disclose U.S. classified information to foreign interests are based on a determination that release is in support of a lawful and authorized U.S. Government purpose. Prior to disclosure of U.S. classified information or material to foreign interests, the U.S. Government shall request and receive a security assurance from the responsible foreign government. Transfer of classified material to a foreign interest shall be through established transmission channels that are approved by the governments involved (government-to-government channels). Receipts shall be obtained for information that is classified Confidential and above.

1302. GOVERNING FEDERAL LAWS. The transfer of defense articles and services, or related technical data, to a foreign person, whether within or outside the United States, or the movement of such material or information to any destination outside the legal jurisdiction of the United States, constitutes an export. Depending on the nature of the material or information, most exports are governed by either the Arms Export Control Act (AECA) (22 U.S.C. 2776 et seq.) or the Export Administration Act (EAA) (P.L. 96-72, as amended). The Defense Authorization Act of 1984 (P.L. 98-94) authorizes the Secretary of Defense to withhold from public disclosure unclassified militarily critical technical data having a military or space application which is possessed or controlled by the Department of Defense (DOD). Other laws that apply to the export of technical data are listed below:

a. Are inherently military in nature and are controlled by the International Traffic in Arms Regulation (ITAR), 22 CFR 120.1-130.17 (1987).

b. Have both military and civilian uses and are controlled by the Export Administration Regulation (EAR), 15 CFR 368.1-399.2 (1987).

1303. FOREIGN GOVERNMENT INFORMATION (FGI). FGI refers to information that is: (1) provided to the United States by a foreign government or governments, an international organization of governments, or any element thereof with the expectation expressed or implied, that the information, the sources of the information, or both, are to be held in confidence; or (2) produced by the United States pursuant to, or as

a result of, a joint arrangement with a foreign government or governments, an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both are to be held in confidence.

1304. CLASSIFICATION MARKINGS ON FGI. Foreign government designations for classified information generally parallel U.S. security classification designations. However, some foreign governments have a fourth level of classification, "RESTRICTED," for which there is no equivalent U.S. classification designation. If FGI is received and the classification and the country of origin are in a language other than English, the equivalent U.S. classification or the designation "RESTRICTED," the country of origin, and the notation "FOREIGN GOVERNMENT INFORMATION," shall be marked on the material, in English. See chapter 6, paragraphs 633 and 634.

1305. MARKING U.S. DOCUMENTS THAT CONTAIN FGI. U.S. documents that contain extracts of foreign government classified information shall be marked on the cover "FOREIGN GOVERNMENT INFORMATION." In addition, the portions shall be marked to identify the classification level and the foreign country of origin. "R" shall be used for portion marking "RESTRICTED" information. For example, (U.K.-C), (U.K.-R), and (German-C). The "Declassify On" line shall contain the following notation, Declassify on: November 14, 2004 or Declassify on: X5 to show that the document reveals FGI or if the document containing this information is exempted from automatic declassification. See appendix 4, section 10-3.

> NOTE: A U.S. document marked as described in this paragraph cannot be downgraded below the highest level of foreign government information contained in the document and it cannot be declassified without the approval of the foreign government involved.

1306. INFORMATION CLASSIFIED BY A FOREIGN ENTITY. FGI classified by a foreign entity shall either retain its original classification designation or be marked with an equivalent U.S. classification designation.

1307. CLASSIFYING INFORMATION PROVIDED BY A FOREIGN ENTITY WITH AN OBLIGATION TO MAINTAIN CONFIDENTIALITY. FGI that is not classified but is provided to the FAA with the expressed or implied obligation to hold it in confidence shall be assigned a national security classification. The procedure for making a classification decision described in chapter 2 of this order does not apply to FGI. When determining the most appropriate level of classification for information in this category, careful consideration must be given to the sensitivity of the subject matter and the impact of its unauthorized disclosure upon both the United States and the originating foreign government or international organization. EO 12958 states that a presumption of damage to the national security in the event of unauthorized disclosure

of FGI will be the guiding force in such matters. Therefore, this type of information shall be classified at least CONFIDENTIAL. Higher levels of classification shall not be assigned without prior approval of the SSE.

1308. DURATION OF CLASSIFICATION FOR FGI. FGI is exempt from declassification requirements of U.S. classified information. Unless guidelines have been developed in consultation with the Archivist of the United States, the Department of State, and the foreign government involved, FGI shall not be assigned a date or event for declassification.

1309. CLASSIFICATION MARKING FOR FGI. Foreign security classifications generally parallel U.S. classifications. If the classification of a foreign government document is shown in English, no additional marking is required. If the foreign classification is not marked in English, the equivalent U.S. designation shall be entered on the material. If there is any doubt as to the correct classification, guidance shall be requested from the SSE.

1310. USE OF "RESTRICTED" MARKING. Certain foreign governments use a fourth classification designation of "RESTRICTED" for which there is no equivalent United States classification. The notation "This classified material is to be safeguarded in accordance with Order 1600.2" shall be shown on the face of the document. FGI that is marked "RESTRICTED" shall be protected as U.S. CONFIDENTIAL except that such information may be stored in locked filing cabinets, desks, or other similar containers under the control of persons authorized access to the information. The safeguarding provided shall be sufficient to prevent uncontrolled access by unauthorized persons. If foreign government "RESTRICTED" information is included in an otherwise unclassified FAA document, the document shall be marked CONFIDENTIAL and all provisions of chapter 6 of this order shall apply.

1311. SAFEGUARDING.

a. FGI or material classified TOP SECRET, SECRET, or CONFIDENTIAL shall be safeguarded in the same manner as required by this order for U.S. classified information or material of an equivalent classification level. To avoid inadvertent compromise, foreign government classified material should be stored to the extent practicable in a manner that will avoid commingling with another government's material.

b. Foreign government RESTRICTED information shall be safeguarded in a manner that will preclude open publication, access, or use for other than official government purposes. RESTRICTED documents may be stored in locked filing cabinets, desks, or similarly secured containers that will prevent access by unauthorized personnel.

1312. DISCLOSURE LIMITATIONS. FGI shall not be disclosed or disseminated to nationals of a third country (including intending citizens) or to any other third party, nor be used for other than the purpose for which it was provided without prior written consent of the foreign government.

1313. TRANSMISSION. FGI shall be transmitted by FAA personnel in the same manner as required by this order for U.S. classified information of an equivalent classification. Foreign government RESTRICTED information shall be transmitted in the same manner as U.S. CONFIDENTIAL information. Transmission of foreign government classified information and material including RESTRICTED to areas outside the United States shall be through government-to-government channels.

1314. REPRODUCTION AND DISPOSITION/DESTRUCTION.

a. Reproduction of foreign government material shall be limited to that which is necessary to accomplish the specific official purpose for which the information was provided.

b. Foreign government classified material shall be returned to the foreign government that provided the information upon completion of the official purpose for which the information was provided unless the information is destroyed or retention has been authorized by the originating foreign government. Foreign government classified information shall be destroyed in the same manner required by this order for United States material of an equivalent classification. Destruction certificates shall be executed for foreign government classified material in the same manner as United States classified material of the same classification level. RESTRICTED material does not require a destruction certificate.

1315. LOSS, COMPROMISE, OR SUSPECTED COMPROMISE. The loss, compromise, or suspected compromise of FGI shall be promptly reported to the SSE. In overseas locations, a report shall also be provided to the appropriate Department of State Regional Security Officer (DOS/RSO).

1316. CONTROL OF NORTH ATLANTIC TREATY ORGANIZATION (NATO) MATERIAL. NATO has issued security regulations for the protection of classified material belonging to its organization. These regulations are applicable to every member state of the NATO and require that each member designate a National Security Authority to ensure the security of NATO information within that member nation's jurisdiction. A Central U.S. Registry for NATO has been established under the Secretary of the Army. This is the main receiving and dispatching authority for the United States for NATO material. A system of subregistries or control points is established within each agency through which the material is received from the Central U.S. Registry and internally disseminated. The Secretary of Defense has been appointed the National Security Authority for the United States. The Secretary of Defense as the National Security

Authority has issued USSAN Instruction 1-69, Implementation of NATO Security Procedures. The current edition of this instruction is effective within the FAA and, together with this order, shall provide guidance for the control and protection of NATO classified material in the custody of the FAA.

1317. FAA NATO CONTROL POINT. The Internal Security Division, ACO-400, is the NATO control point for the FAA. All classified NATO material for the FAA should be transmitted to the ACO-400 SCP, FAA Headquarters, Washington, DC. No person shall be given access to NATO information unless he/she has been specifically authorized such access and has been briefed on his/her responsibilities to protect the information. A formal written authorization for access to NATO material is required in addition to any other security clearance or authorization the individual may have. The latest edition of Order 1600.1, Personnel Security Program, contains procedures for the issuance of this access authorization. The custodian of the ACO-400 SCP shall maintain a current roster of all individuals within the FAA who are authorized to receive NATO material. The custodian shall ensure that NATO material is released only to those FAA personnel whose names appear on the roster. Prior to release of NATO classified information to any individual, the custodian of the ACO-400 SCP shall ensure that the prospective recipient can provide the required storage, safeguarding, and control of the information required by this order.

1318. CONTROL OF CLASSIFIED INFORMATION RECEIVED IN THE UNITED STATES FROM INTERNATIONAL ORGANIZATIONS OTHER THAN NATO. Documents or material transmitted to the FAA bearing classification markings of another country or international group other than NATO shall be routed to the ACO-400 SCP for processing. ACO-400 shall determine the requirements that apply for safeguarding, distribution, and control of such documents based on the classification level and types of material concerned. ACO-400 shall ensure that these procedures are followed throughout any distribution that is made to offices or activities within the FAA.

1319. CONTROL OF CLASSIFIED INFORMATION RECEIVED OVERSEAS FROM INTERNATIONAL ORGANIZATIONS OTHER THAN NATO. If classified material from international organizations is received by any FAA element overseas, it shall be the responsibility of the individual or office receiving such material to notify the SSE by the most expeditious means. The SSE shall take appropriate action to ensure that the document/material is controlled, safeguarded, and transmitted or stored in accordance with the provisions of this order for U.S. classified material of equivalent classification level. If, for any reason, there is a delay in the notification to the SSE, the FAA official responsible for the document/material shall seek guidance from the nearest DOS/RSO concerning safeguarding procedures to be followed until the SSE can be contacted. The document/material shall be safeguarded as classified until specific instructions are received from the SSE.

1320.-1399. RESERVED.

CHAPTER 14. VISITOR CONTROL

1400. GENERAL. The term "visitor" in this order applies to all personnel including FAA contractors and other personnel who are not attached to, employed by, or on temporary duty (TDY) orders to the FAA office, activity, or facility concerned. Personnel who are assigned on TDY orders are considered as attached to a facility and not visitors even though they may not be directly employed by that particular activity.

1401. VISITS BY FAA EMPLOYEES TO OTHER GOVERNMENT FACILITIES. Arrangement for visits by FAA personnel to other government agencies and contractors shall be made sufficiently in advance of the visit to permit processing of the visit request. Form DOT F 1630.5, Visit Clearance, shall be prepared by the FAA office initiating the visit and provided to the servicing security element (SSE) for review, certification of security clearance, and transmittal to the facility.

1402. REQUIREMENTS FOR USE OF DOT F 1600.15 OR CONSOLIDATED PERSONNEL MANAGEMENT INFORMATION SYSTEM (CPMIS). DOT F 1600.15 shall be used for notification of visits requiring access to classified information for intra-FAA and other organizations. Region/center SSE's with access to the CPMIS may verify security clearance data on FAA employees using CPMIS instead of using DOT F 1630.5. The office or facility being visited shall notify the SSE as soon as they are aware of a visit which requires access to classified information so that the security clearance data in the CPMIS can be verified. The name, social security number, facility to be visited, level of access required, and dates of visit shall be provided to the SSE. The SSE shall confirm the security clearance data in the CPMIS and will transmit the information to the activity or facility to be visited.

1403. VISITOR CATEGORIES AND PROCESSING PROCEDURES. For the purpose of this order, visitors to FAA facilities are divided into five general groups. These groups are listed in the following paragraphs together with the appropriate visit request procedures for each group.

a. Group 1 includes Executive Branch personnel of the Government who normally have daily or frequent contact with the FAA activity to be visited and are personally known by the facility personnel. No formal visit notifications are required for this group, but if access to classified information is required during the visit, each person being visited is responsible for ensuring the visitor has a need to know and has the appropriate security clearance.

b. Group 2 includes all Executive Branch personnel who do not fall under Group 1. For this group a formal visit request is required. The visit request may be approved by the FAA head of the office or activity being visited or his or her designee subject to the requirements of this order. A certificate of clearance contained in an official visit

request from another Government agency should be accepted. The visit request shall contain the following information as a minimum:

(1) Full name; military rank, if appropriate; title, or position.

(2) Citizenship, date, and place of birth.

(3) Employer or sponsor, if other than the originator of the visit request.

(4) Name and address of the activity to be visited, if other than the address on the visit application.

(5) Date, time, and duration of proposed visit.

(6) Description of purpose of visit in detail, including estimated degree of access required.

(7) Security clearance status of the visitor and the clearing agency.

(8) Names of persons to be visited, if known.

c. Group 3 includes all contractor employees cleared under the DOD Industrial Security Program. Contractor employees in this group should have their requests submitted by their employer to the heads of FAA offices or specific activities to be visited. If access to classified information is involved, the Government contracting officer must certify that the visit and release of classified information is essential. Visits in this category may be approved by the head of the office or activity being visited or his/her designee. A cleared contractor's certification of the clearance of the employee up to CONFIDENTIAL may be accepted without further confirmation. Visit requests should contain the following information as a minimum:

(1) Name and address of activity to be visited.

(2) Name and title of person(s) to be visited, if known.

(3) Name of visitor, date and place of birth, and citizenship.

(4) Job title or position of the visitor.

(5) Contractor's certification of the clearance status of the visitor including level, date, and issuing authority.

(6) Purpose of and justification for the visit, including the contract or program the visitor is working on and specific classified information required during the visit, if known.

(7) Date(s) of proposed visit(s) or period during which request is valid.

(8) Name and address of contractor or user agency activity.

(9) Level of contractor's facility clearance and date granted.

(10) Name and address of contractor's cognizant security office, including telephone number, if known.

NOTE: The contractor's cognizant security office would have no record of contractor-granted CONFIDENTIAL clearances.

d. Group 4 includes U.S. citizens on unofficial business visits. These types of visits may be approved by the head of the FAA offices or activities being visited or his or her designee. Visitors in this group shall not be granted access to classified information, oral or visual, without the prior written approval of ACS-1.

e. Group 5 includes foreign national visitors and foreign representatives. Visitors in this group shall not be granted access to classified information. Whenever an office or facility manager first becomes aware of a request for foreign nationals or foreign representatives to visit his or her area, the manager should consult the latest edition of Order 1600.65, Facility Visits by Foreign Nationals and Representatives. This order contains the procedures and requirements concerning all such visits.

1404. IDENTIFICATION REQUIREMENTS FOR VISITORS TO FAA FACILITIES. Visitors shall present sufficient identification to satisfy the office being visited. If there are any questions, the Government agency, contractor, or sponsor shall be contacted for confirmation of identity. Unique problems shall be referred to the SSE.

1405. REQUIREMENT FOR MAINTENANCE OF A VISITOR LOG. An FAA Form 1600.8, Visitor Log, shall be maintained by the office, activity, or facility being visited. Visitors should be required to provide the information on the FAA Form 1600.8 and to sign in upon arrival and sign out upon completion of the visit.

1406. MOVEMENT RESTRICTIONS AND ESCORT REQUIREMENTS. The manager of the office, activity, or facility responsible for the classified information shall ensure that visitors are given access only to that classified information to which they have been granted access authorization. Visitors shall be escorted in areas where they could otherwise gain unauthorized access to classified information. The designated escort shall be a responsible, appropriately cleared FAA employee who is aware of the access limitations of the visitor and the restrictions placed on the visitor's movements. Visits of tour groups and guests to FAA activities shall be guided by an appropriate escort.

1407. BADGING REQUIREMENTS FOR VISITORS. If an FAA facility uses a visitor badging system, the badges shall be distinctive so that it is readily apparent that the wearer is a visitor.

1408. RESTRICTIONS ON PHOTOGRAPHY. Photography shall not be permitted on or within an FAA facility without the prior permission of the facility manager. Photographs are prohibited in areas where classified information is processed, handled, or displayed unless accomplished in accordance with procedures specifically approved by the SSE.

1409. RESTRICTIONS ON USE OF ELECTRONIC RECORDING DEVICES. The use of audio, video, or other types of electronic recording equipment within an FAA office, activity, or facility is prohibited without the prior permission of the facility manager.

1410. REPORTING UNUSUAL VISITOR INTEREST. If a visitor expresses an unusual interest in information that he or she is not authorized to receive or expresses beliefs that are inimical to the best interests of the United States, the head of the FAA office, activity, or facility shall report the circumstances to the SSE. The SSE shall refer the information through ACO-400 to M-70. The information provided to the SSE shall include the following information:

a. Full name and title or position of visitor.

b. Nationality.

c. Sponsor.

d. Authority for visit.

e. Items of particular interest to the visitor.

f. General type of questions asked.

g. Expressed object of visit.

h. Estimate of the real object of the visit.

i. General estimate of ability, intelligence, and technical knowledge of the visitor.

j. Exactly what was shown, explained, and refused.

1411. VISITS BY FAA EMPLOYEES TO FAA AND OTHER GOVERNMENT FACILITIES. Arrangements for visits by FAA employees to other FAA facilities, government agencies, and contractors shall be made sufficiently in advance of the date of the visit

to permit processing of the visit request. The information may be provided by telephone and be confirmed in writing. An employee may not hand-carry his or her own visit request.

a. Form DOT F 1630.5, Visit Clearance, shall be prepared for notification of visit and clearance certification for FAA employees requiring access to classified information. The form shall be prepared by the office initiating the visit and provided to the SSE for review, certification of security clearance, and transmittal.

b. For visits by FAA employees to FAA facilities, regions, and centers, SSE's may access the CPMIS to verify security clearance data on the employee(s) instead of using Form DOT F 1630.5.

c. The manager of the office or facility being visited shall notify the SSE as soon as he or she is aware of a visit which requires access to classified information so that security clearance data in the CPMIS can be verified. The name, social security number, identification of the facility to be visited, the level of access to classified information that will be required, and the dates of the visit shall be provided to the SSE. The SSE shall obtain a hard copy of the clearance confirmation data produced by the CPMIS and ensure that it is transmitted to the facility to be visited.

1412.-1499. RESERVED.

CHAPTER 15. COMPROMISES AND SECURITY VIOLATIONS

1500. GENERAL. The policies and procedures in this order and related security directives are intended to prevent the compromise of classified information. Failure to follow these procedures in the handling and dissemination of classified information could subject the classified material to loss or compromise. An infraction of a specific procedure or requirement for safeguarding or handling classified material may not subject the information to compromise in one instance, but under different circumstances could result in loss or compromise. For this reason ALL violations of the provisions of this order as well as other directives applicable to the safeguarding of classified information shall be reported.

1501. COMPROMISE OF CLASSIFIED INFORMATION. Examples of instances in which compromise shall be presumed include, but are not limited to, discussion of classified information on nonsecure telephones, disclosure of classified information to uncleared persons, and the actual loss of classified information. Examples of possible compromise include, but are not limited to, leaving a security container used for classified storage open and unattended and transmitting classified information via unauthorized channels.

1502. REPORTING SECURITY VIOLATIONS. Any FAA employee, military personnel, or other person having knowledge of a violation of security regulations, or of the loss, unauthorized disclosure, or actual or possible compromise of classified information shall immediately report the details to his or her immediate supervisor or to the SSE. When the report is submitted to the immediate supervisor, the supervisor shall ensure that the matter is referred without delay to the SSE. Upon receipt of the report and depending upon the nature of the violation, the SSE, in coordination with the responsible individual or manager, shall endeavor to recover the material and provide adequate safeguarding and shall ensure that all documentation and evidence of tampering regarding the loss or compromise is preserved intact.

1503. ADMINISTRATIVE INQUIRIES. When a security violation consists of a minor deviation from the requirements of this order, an administrative inquiry shall be conducted by the manager of the office or activity responsible for the classified information or the SSE. If, as a result of this inquiry, it is determined that a loss of classified material did not occur or that the possibility of compromise was remote, the result of the inquiry and a statement of corrective action taken as well as a statement of any disciplinary action shall be reported to the SSE within 10 calendar days after the date of discovery of the violation.

1504. INVESTIGATIVE REQUIREMENTS IN INCIDENTS INVOLVING PROBABLE COMPROMISE. If the security violation is such that it appears that an actual compromise of classified information has occurred or that the likelihood of an actual compromise cannot be discounted, the SSE shall immediately report the full details of

the matter to ACO-400. ACO-400 shall, depending upon the circumstances and the sensitivity of the affected information, notify the originating agency of the fact that compromise of the information is likely, and shall provide a copy of this notification to ACO-400 and M-70. The reporting SSE shall immediately initiate a comprehensive investigation to determine the following: the circumstances of the violation: where, when, and how the violation occurred; who was responsible; the description and classification of the information; and the measures taken to recover lost or misplaced material. The report of investigation shall evaluate the probability of compromise and the significance of the incident. The report shall be submitted to the head of the activity where the incident occurred and a copy shall be submitted to ACO-400. ACO-400 shall take appropriate action to forward the report to the originator of the classified material and to M-70.

1505. CORRECTIVE ACTIONS REQUIRED SUBSEQUENT TO ACTUAL OR POSSIBLE LOSS OR COMPROMISE OF CLASSIFIED INFORMATION ORIGINATED BY THE FAA. When an FAA office or activity that has originated classified information is informed that the information has been subjected to compromise, it shall initiate appropriate action to change portions of plans, programs, or operations to minimize adverse impacts from the compromise. A classification review of the information shall be conducted to determine if it should be regraded or declassified. Notification of changes shall be provided to holders of the material. All actions taken shall be coordinated with the SSE. Corrective actions are subject to review by the Departmental Security Review Committee.

1506. ADMINISTRATIVE AND DISCIPLINARY ACTIONS. When a loss or compromise has occurred, the manager of the office or facility responsible for the information shall take immediate corrective action to prevent the occurrence of similar violations. Such actions may include but are not limited to: changes in local practices regarding controlling classified information; intensification of security briefings; and administrative or disciplinary action.

a. In determining the disciplinary action to be taken, officials shall be guided by an overall assessment of the occurrence including the seriousness of the violation, the sensitivity of the information subjected to compromise, and evidence of disregard or continuing disregard of security regulations.

b. Administrative actions are separate from criminal penalties for violation of statutes dealing with unauthorized release of classified information. If individual responsibility for the violation cannot be determined, but the facts indicate that a supervisor or other official allowed conditions to exist which led to the violation, the responsibility shall be placed on that official.

1507. MARKING ADMINISTRATIVE INQUIRIES AND REPORTS OF INVESTIGATION. Reports of security violations, formal investigations, administrative inquiries, and letters of discipline shall not be classified unless the report itself contains classified information. Reports may be given the protective marking - "FOR OFFICIAL USE ONLY." If classified information appears in the public media, reports of such instances shall be classified at the same level as the information in the public media until an evaluation is made by an OCA concerning whether or not the information will be downgraded or declassified. If the determination is made to retain the classification, the incident report shall remain classified. Additionally, an incident report which may assist an unauthorized person in finding lost or missing classified information shall remain classified.

1508. COMPROMISES OF CRYPTOGRAPHIC INFORMATION. Possible compromises of classified cryptographic material shall be reported to the SSE by the most expeditious secure means and handled in accordance with the provisions of the latest edition of Order 1600.8, Communications Security (COMSEC) and Electronic Key Management Systems (EKMS).

1509. COMPROMISE OF CLASSIFIED INFORMATION ORIGINATED BY A FOREIGN GOVERNMENT. M-70 will ensure that appropriate action is taken when classified information originated by a foreign government or belonging to an international organization has been subjected to compromise while in the custody of the FAA. All such incidents shall be reported to ACO-400 immediately, through the SSE, and ACO-400 shall forward the information to M-70 for appropriate action.

1510.-1599. RESERVED.

CHAPTER 16. MISCELLANEOUS INFORMATION

1600. OPERATIONS SECURITY. The general aim of Operations Security (OPSEC) is to promote mission effectiveness by preserving essential secrecy about U.S. intentions, capabilities, and current activities when the requirements of this order for safeguarding classified material and information require enhancement. OPSEC is directed to the protection of unclassified intelligence indicators when necessary to preserve the security integrity of a classified program. While the FAA does not handle large volumes of classified or national security information on a regular basis, there are specific missions and programs that do require this type of material. The integrity of classified and sensitive FAA programs may be compromised whenever open sources (such as technical articles, press releases, National Technical Information Service publications, the Congressional Record, Commerce Business Daily, or contract awards) and detectable activities (such as communications, logistics actions, research and development, and test activities) provide information that can be pieced together by unauthorized persons and can result in actions harmful to U.S. interests. OPSEC thus encompasses activities which are unique to the OPSEC process to include the following:

a. Determination through threat/vulnerability analysis, whether there are unacceptable/undesirable intelligence indicators and what they are.

b. Developing and implementing countermeasures to eliminate or minimize such indicators.

1601. TEMPEST. TEMPEST is an unclassified short name referring to investigations and studies of compromising emanations. TEMPEST is often used synonomously for the term "compromising emanations." Compromising emanations are unintentional intelligence-bearing signals which, if intercepted and analyzed, will disclose classified information when it is transmitted, received, handled, or otherwise processed by any information processing equipment. Emanations are either acoustic or electric and may be transmitted through free space or solid conductive mediums.

a. TEMPEST problems can be reduced or eliminated through the use of techniques prescribed in National Telecommunications and Information Systems Security Instruction (NTISSI) 7000, TEMPEST Countermeasures for Facilities. Information concerning TEMPEST and TEMPEST requirements can be obtained from ACO-400.

b. Any equipment which electromechanically or electronically processes, introduces, converts, or otherwise manipulates any form of information is "information processing equipment." The following equipment is typical: electric typewriters, reproduction equipment, word processors, composing and editing equipment, video

displays, automated information systems, telecommunications equipment and systems, including teletype, facsimile, and cryptographic equipment, and all interfaces, power sources, and interconnecting paths which are part of the system or equipment.

1602. SECURE TELEPHONE UNIT (STU-III). Within recent years, the FAA has acquired and placed into service increasing numbers of secure telephone units, STU-III's. These are a relatively new family of secure telephone equipment sponsored by the National Security Agency (NSA), which provide low cost, user-friendly, secure telephones that are the size of conventional telephones and are compatible with existing communications systems. The Emergency Operations Staff, ADA-20, is the controlling authority for acquisition and placement of STU-III telephones within the FAA. Security requirements for STU-III equipment are contained in the NSA-produced User Manual, instructions provided by ADA-20, and in the latest edition of Order 1600.8, Communications Security (COMSEC) And Electronic Key Management Systems (EKMS).

1603.-1699. RESERVED.

CHAPTER 17. SECURITY EDUCATION

1700. GENERAL. A continuing and meaningful security education program relevant to the operations of the FAA shall be established and maintained. The security education program shall include all personnel entrusted with classified information regardless of their position, rank, or grade. Care shall be exercised to ensure that the program does not evolve into perfunctory compliance with formal requirements.

1701. RESPONSIBILITIES FOR SECURITY EDUCATION.

a. Washington headquarters. The Office of CAS Operations, ACO, is responsible for ensuring that the provisions of this chapter are met for FAA elements and personnel in the Washington headquarters. The Internal Security Division, ACO-400, is the focal point within ACO for matters relating to security education.

b. Regions and centers. The CAS division or staff within each region and center in the continental United States and in overseas areas as the SSE is responsible for ensuring that the provisions of this chapter are met within their respective areas of jurisdiction.

c. FAA Offices and Services. Any office, service, or element within the FAA that has the responsibility for handling, processing, storing, transmitting, or developing classified information is responsible for coordinating with the appropriate SSE to ensure that all personnel responsible for classified material are trained in accordance with this chapter.

1702. PROGRAM DESIGN. As a minimum, the security education program shall be designed to:

a. Advise personnel of the need for protecting classified information, and the adverse effects to the national security that could result from unauthorized disclosure of classified information.

b. Emphasize the personal responsibility that each FAA employee has for properly safeguarding classified, sensitive, and proprietary information in his or her possession.

c. Indoctrinate personnel in the principles, criteria, and procedures for classification, downgrading, declassification, and marking of classified documents in accordance with this order.

d. Alert personnel to the prohibitions and penalties that apply to the improper use and abuse of the classification system.

e. Familiarize personnel with the procedures for challenging classification decisions and any specific security requirements of their particular assignment.

f. Advise personnel of the prohibitions against discussing classified information over the telephone or in the presence of unauthorized persons.

g. Inform personnel of the disciplinary actions that may result from violation, neglect, or disregard of E.O. 12958 or successor directives, any implementing directive such as ISOO Directive Number 1, or this order.

h. Advise personnel that the individual having knowledge, possession, or control of classified information has the responsibility for determining - prior to the release of the information to another individual that: (1) the intended recipient has been appropriately cleared for access to the information, (2) a need to know exists for the information in order that the recipient may perform his/her official duties, and (3) the recipient can properly protect or store the information.

1703. INDOCTRINATION BRIEFING. An initial briefing of new personnel being assigned to duties requiring access to classified information shall be provided by ACO-400 in the Washington headquarters and by the appropriate SSE in regions, centers, and overseas areas.

1704. REFRESHER BRIEFING. FAA personnel who have had access to classified information shall be given a briefing as a defensive measure prior to foreign travel to alert them of the possibility that they may be targeted by foreign intelligence services in an effort to obtain the classified knowledge they possess. Individuals who frequently travel, attend meetings, or host meetings of foreign visitors need not be briefed for each such occasion. A thorough counterintelligence awareness briefing provided by the SSE at least once a year shall normally be sufficient.

1705. REPORTING CONTACTS WITH FOREIGN NATIONALS. FAA employees having access to classified information shall promptly report to the SSE for appropriate action all contacts with individuals of any nationality, either within or outside the scope of the employee's official activities in which there is an attempt on the part of the individual to do any of the following:

a. Use the employee to seek illegal or unauthorized access to classified or otherwise sensitive information.

b. Exploit the employee for intelligence purposes.

1706. PROCESSING REPORTS OF CONTACTS WITH FOREIGN NATIONALS. Upon receipt of a report of contact with foreign nationals from an FAA employee, the SSE will review and evaluate the reported information. Any facets or circumstances of a

reported contact with a foreign national which appear to indicate an attempt, intention, or reasonable potential to obtain unauthorized access to classified, sensitive, or proprietary information or technology, or that indicate the possibility of continued contact with the foreign national for such purposes, shall be promptly reported to M-70 through ACS-1. M-70 shall in turn take the appropriate action to notify the FBI in the case of employees located in the United States. In overseas locations, the SSE shall promptly report the contact information to the Regional Security Officer of the Department of State, with an information copy of the report forwarded to M-70 through ACS-1. Information concerning reports of contacts by foreign nationals shall be transmitted electronically only by secure transmission media.

1707. DEBRIEFINGS. Personnel who transfer, resign, or separate shall be debriefed and return all classified material in their custody to their Classified Information Account Custodian (CIAC) or Security Control Point (SCP). FAA personnel who leave the employ or service of the FAA, or who anticipate a temporary separation of 60 days or more, and who have been authorized access to classified information, shall be debriefed and shall execute a Security Termination Statement.

1708.-1799. RESERVED.

APPENDIX 1. GLOSSARY OF TERMS

Access. The ability and opportunity to obtain knowledge of classified national security information.

NOTE: A person may have access to classified information by being in an area where such information is kept if security precautionary measures are not taken to prevent the person from gaining knowledge of the classified information.

ACIAC. FAA acronym that stands for alternate classified information account custodian.

AIS Security. All security safeguards needed to provide an acceptable level of protection for automated information systems and the classified data processed. Includes all hardware or software functions; characteristics; and mechanisms; operational accountability and access control procedures at the computer and remote terminal facilities; and management constraints, physical structures, and devices needed to provide required levels of protection for classified information in any state of storage, processing, display, or communications within the AIS.

Approved Access Control Device. An access control device that meets the requirements of this order and has been approved by the SSE or ACO-300 for the intended security application.

Approved Alarm System. An alarm system that meets the requirements of this order and has been approved for the intended security application by the SSE or ACO-400.

Approved Built-in Combination Lock. A combination lock, equipped with a top reading dial, that conforms to Underwriters' Laboratories, Inc., Standard Number UL 768, Group 1R.

NOTE: New security containers purchased from the GSA Schedule are required to have an approved electronic lock.

Approved Combination Padlock. A three position dial-type changeable combination padlock listed on the GSA Qualified Products List as meeting the requirements of Federal Specification FF-P-110.

Approved Electric, Mechanical, or Electromechanical Device. An electric, mechanical, or electromechanical device that meets the requirements of this order and is approved for the specific application by the SSE.

Approved Key-Operated Padlock. A padlock, which meets the requirements of MIL-SPEC-P-43607 (shrouded shackle), National Stock Number 5340-00-799-8248, or MIL-SPEC-P43951 (regular shackle), National Stock Number 5340-00-799-8016.

Approved Security Container. A security file container, originally procured from a Federal Supply Schedule supplier that conforms to Federal specifications and bears a "Test Certification Label" on the locking drawer attesting to the security capabilities of the container and lock. Such containers will be labeled "General Services Administration Approved Security Container" on the outside of the top drawer. Acceptable tests of these containers can be performed only by a testing facility specifically approved by the General Services Administration.

Approved Strongroom. A strongroom which has been constructed in accordance with this order and Order 1600.6C, Physical Security Management Program, and has been approved by the SSE for use in safeguarding of classified information.

Approved Vault. A vault which meets the structural requirements of this order and has been specifically approved by the SSE and ACO-400 for the safeguarding of classified information.

Authorized Person. A person who has a need to know of classified information in the performance of official duties and who has been granted a personnel clearance at the required level. The responsibility for determining whether a prospective recipient is an "authorized person" rests with the person who has possession, knowledge, or control of the classified information involved, and not with the prospective recipient.

Classification. The act or process by which information is determined to be classified.

Classification Guide. A document issued by an authorized original classifier that identifies the elements of information, level of classification, and appropriate declassification instructions for specific information to be classified on a derivative basis.

Classification Guidance. This means any instruction or source that prescribes the classification of specific information.

Classified National Security Information. Information that has been determined pursuant to this order or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

Classified Visit. A visit that requires, or is expected to require, access to classified information by the visitor.

Classifier. Any person who makes a classification determination and applies a security classification to information or material. The determination may be an original classification action or it may be a derivative classification action.

Closed Area. A controlled area which meets the requirements of this order and Order 1600.6C and is approved by the SSE for the safeguarding of classified material which, because of its size or nature, cannot be adequately protected by the normal safeguards or stored during non-working hours in approved containers.

Communications Security. Protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government relating to national security and to ensure the authenticity of such communications. COMSEC protection results from the application of security measures to electrical systems which generate, handle, process, or use classified national security or sensitive information and also includes the application of protective measures to COMSEC equipment and keying materials.

Compromise. The disclosure of classified information to persons not authorized access to it.

Confidential. "CONFIDENTIAL" is the designation that shall be applied to material the unauthorized disclosure of which could be reasonably expected to cause damage to the national security. Examples of "damage" include the compromise of information that indicates strength of ground, air, and naval forces in the United States and overseas areas, disclosure of technical information used for training, maintenance, and inspection of classified munitions of war, and revelation of performance characteristics, test data, design, and production data on munitions of war.

Constant Surveillance Service. A transportation protective service provided by a commercial carrier approved to transport CONFIDENTIAL shipments. The service requires constant surveillance of the shipment at all times by a qualified carrier representative. The carrier providing the service must maintain a signature and tally record for the shipment.

Controlled Areas. A general term which for purposes of this order consists of both "Closed Areas" and "Restricted Areas."

Custodian. An individual who has possession of or is otherwise charged with the responsibility for safeguarding or accounting for classified information.

Declassification. The determination that classified information no longer requires, in the interest of classified national security information, any degree of protection against unauthorized disclosure, together with removal or cancellation of the classification designation.

Declassification Event. An event that eliminates the need for continued classification of information.

Derivative Classification. A determination that information is in substance the same as information currently classified and the application of the same classification markings.

Document. Any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed matter, data processing cards, tapes, charts, maps, paintings, drawing, engravings, sketches, working notes, and papers; reproductions of such things by any means or process; and sound, voice, magnetic, or electronic recordings in any form.

Downgrade. A determination that classified information requires, in the interest of classified national security, a lower degree of protection against unauthorized disclosure than currently provided, together with a changing of the classification designation to reflect a lower degree of protection.

File series. Documentary material, regardless of its physical form or characteristics, that is arranged in accordance with a filing system or maintained as a unit because it pertains to the same function or activity.

Foreign Government Information. Information that is: (1) provided to the United States by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the course of the information, or both, are to be held in confidence; or (2) produced by the United States pursuant to, or as a result of, a joint arrangement with a foreign government or governments, an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both are to be held in confidence.

Foreign Interest. Any foreign government, or representative of a foreign government; any form of business enterprise or legal entity organized under the laws of any country other than the United States or its possessions, and any person who is not a citizen or national of the United States (an "intending citizen" and a foreign-owned U.S. company are excluded from the definition of a foreign interest).

Foreign Nationals. All persons not citizens or nationals of the United States.

Formerly Restricted Data. Information removed from the RESTRICTED DATA category upon a joint determination by the Department of Energy (DOE) (or antecedent agencies) and the Department of Defense (DOD) that such information relates primarily to the military utilization of atomic weapons, and that such information can be adequately safeguarded as classified defense information. For purposes of foreign dissemination, however, such information is treated in the same manner as Restricted Data.

For Official Use Only. Information that has not been given a security classification pursuant to the criteria of an Executive order, but which may be withheld from public disclosure under the criteria of the Freedom of Information Act, Title 5, U.S.C., Section 552.

Government-To-Government Channels. The principle that classified information or material will be transferred by government officials through official channels specified by the governments involved.

Graphic Arts. Facilities and individuals engaged in performing consultation, service, or the production of any component or end product which contributes to, or results in, the reproduction of classified information. Regardless of trade names of specialized processes, it includes writing, illustrating, advertising services, copy preparation, all methods of printing, finishing services, duplicating, photocopying, and film processing activities.

Industrial Security. That portion of information security which is concerned with the protection of classified information in the hands of U.S. industry.

Information. Any knowledge that can be communicated or documentary information or material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the U.S. Government.

Information Security. The result of any system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure information the protection of which is authorized by Executive order.

Intelligence. Intelligence is the product resulting from the collection, evaluation, analysis, integration, and interpretation of all available information, which concerns one or more aspects of foreign nations or of areas of foreign operations, and which is immediately or potentially significant to military planning and operations.

Intelligence Information. Information that is under the jurisdiction and control of the Director of Central Intelligence or a member of the intelligence community.

Limited Access Authorization. Security access authorization to CONFIDENTIAL or SECRET information granted to non-U.S. citizens requiring such limited access in the course of their regular duties.

Limited Dissemination. Restrictive controls for classified information established by an original classification authority to emphasize need-to-know protective measures available within the regular security system.

Locked Entrance. An entrance to a closed area or a restricted area that is kept closed and locked at all times except when temporarily unlocked and opened under supervision for the purpose of passing material or authorized personnel into or out of the area.

Material. Any product or substance on or in which information is embodied.

Meeting. (Classified). A conference, seminar, symposium, exhibit, convention, or other gathering during which classified information, or foreign classified information entrusted to the U.S. Government, is disclosed.

Multiple Sources. This is two or more source documents classification guides, or a combination of both.

National of the United States. A national of the United States is: (1) a citizen of the United States, or (2) a person who is not a citizen of the United States, but owes permanent allegiance to the United States. NOTE: 8 U.S.C. Sec 1101(a)(22). 8 U.S.C. Sec 1401(a) lists in paragraphs (1) through (7) categories of persons born in and outside the United States or its possessions who may qualify as nationals of the United States. This subsection should be consulted when doubt exists as to whether or not a person can qualify as a national of the United States.

National Security. The national defense and foreign relations of the United States.

NATO Information. Information bearing NATO markings, indicating the information is the property of NATO, access to which is limited to representatives of NATO and its member nations unless proper NATO authority has been obtained to release outside NATO.

Need to Know. A determination made by the possessor of classified information that a prospective recipient has a requirement for access to, knowledge of, or possession of the classified information in order to perform his or her official mission.

Original Classification. An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure, together with a classification designation signifying the level of protection required. (Only government officials, who have been designated in writing, may apply an original classification to information.)

Original classification authority (OCA). An individual authorized in writing, either by the President or by agency heads or other officials designated by the President, to classify information in the first instance.

Public Disclosure. The passing of classified information and/or material to the public by any means of communication.

Regrade. To assign a higher or lower security classification to an item of classified material.

Representative of a Foreign Interest. A citizen or national of the United States, or an intending citizen to the United States, who is acting as a representative of a foreign interest. (See "Foreign Interest.")

Restricted Area. As it is used in this order, a Restricted Area is a controlled area with unescorted access limited to persons having an operational need to be in the area.

Restricted Data. All data or information concerning: (1) design, manufacture, or utilization of atomic weapons; (2) the product of special nuclear material; or (3) the use of special nuclear material in the material production of energy, but not to include data declassified or removed from the Restricted Data category pursuant to Section 142 of the Atomic Energy Act .

SECRET. The designation that shall be applied only to information or material the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security. Examples of "serious damage" include disruption of foreign relations significantly affecting the national security, significant impairment of a program or policy directly related to the national security, revelation of significant military plans or intelligence operations, and compromise of significant scientific or technological developments relating to national security.

Security. As it is used in this order, "security" means the safeguarding of information classified TOP SECRET, SECRET, and CONFIDENTIAL against unlawful or unauthorized dissemination, duplication, or observation.

Security Clearance. An administrative determination that an individual is eligible, from a security point of view, for access to classified information of the same or lower category as the level of the personnel security clearance being granted.

Security Violation. Failure to comply with the policy and procedures established by this order which reasonably could result in the loss or compromise of classified information.

Sensitive But Unclassified (SBU) Information. Information which warrants a degree of protection and administrative control that meets the criteria for exemption from public disclosure set forth under the provisions of Title 5, United States Code Sections 552 and 552a, as defined in The Freedom of Information Act and the Privacy Act.

Sensitive Compartmented Information (SCI). All intelligence information and material that requires special controls for restricted handling within compartmented channels and for which compartmentation is established.

Servicing Security Element (SSE). The headquarters, region, or center organizational element which is responsible for providing security services to a particular activity. This refers to the Civil Aviation Security Divisions (CASD) and the Technical Center Security Staff.

Signature and Tally Record. A record that is an integral part of Protective Security Service and Constant Surveillance Service and is designed to provide continuous accountability and custody of a shipment from point of pickup to delivery to the consignee. For commercial air shipments, a signature is not required from the flight crew or attendees of the carrier's aircraft.

Source Document. An existing document that contains classified information that is extracted for inclusion in another document. The classified information that is extracted is incorporated, paraphrased, restated, or generated in new form into the source document.

Technical Data. Information governed by the International Traffic in Arms Regulation (ITAR) and the Export Administration Regulation (EAR). The export of technical data that is inherently military in character is controlled by the ITAR, 22 C.F.R. Sec 120.1-130.17 (1987). The export of technical data that has both military and civilian uses is controlled by the EAR, 15 CFR Sec 368.1-399.2 (1987).

TOP SECRET. The designation that shall be applied only to information or material the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security. Examples of "exceptionally grave damage" include armed hostilities against the United States or its allies, disruption of foreign relations vitally affecting the national security, the compromise of vital national defense plans or complex cryptologic and communication intelligence systems, the revelation of sensitive intelligence operations, and the disclosure of scientific or technological development vital to national security.

Transmission. The sending of information from one place to another by radio, microwave, laser, or other nonconnective methods, as well as by cable, wire, or other connective medium. Transmission also includes movement involving the actual transfer of custody and responsibility for a document or other classified material from one authorized addressee to another.

Unauthorized Person. A person not authorized to have access to specific classified information in accordance with the requirements of this order.
Example: United States and its territories. The 50 states; the District of Columbia; the Commonwealth of Puerto Rico; the Commonwealth of Northern Mariana Islands; the Trust Territory of the Pacific Islands-the Republic of Palau; and the Possessions - Midway and Wake Islands.

United States. The 50 states and the District of Columbia.

Upgrade. A determination that certain classified information, in the interest of national security, requires a higher degree of protection against unauthorized disclosure than currently provided, coupled with a changing of the classification designation to reflect such a higher degree of protection.

Working Hours. The period of time when (1) there is present in the specific area where classified material is located a work force on a regularly scheduled basis, as contrasted with employees working within an area on an overtime basis outside the scheduled workshift; and (2) the number of employees in the scheduled work force is sufficient in number and so positioned to be able to detect and challenge the presence of unauthorized personnel. This would exclude therefore, janitors, maintenance personnel, and other individuals whose duties require movement throughout the facility.

APPENDIX 2. FORMS

DOT F 1600.22	Destruction of Classified Record
DOT F 1600.4	Classified Material Record
DOT F 1600.32	Top Secret Disclosure Record
DOT F 1600-35	Classified Document Register
DOT F 1630.5	Visit Clearance
FAA F 1600.8	Visitor Log
FAA F 1600.49	No Classified Reproduction Authorized
FAA F 2833	Report of Security Violation
SF 86	Questionnaire for National Security Positions
SF 87	Fingerprint Chart
SF 135	Record Transmittal and Receipt Form
SF 312	Classified Information Nondisclosure Agreement
SF 700 (NSN 7540-01-214-5372)	Security Container Information
SF 701 (NSN 7540-01-213-7899)	Activity Security Checklist
SF 702 (NSN 7540-01-213-7900)	Security Container Check Sheet
SF 703 (NSN 7540-01-213-7901)	TOP SECRET Cover Sheet

SF 704 (NSN 7540-01-213-7902)	SECRET Cover Sheet
SF 705 (NSN 7540-01-213-7903)	CONFIDENTIAL Cover Sheet
SF 706 (NSN 7540-01-207-5536)	TOP SECRET Label
SF 707 (NSN 7540-01-207-5537)	SECRET Label
SF 708 (NSN 7540-01-207-5540)	CONFIDENTIAL Label
SF 709 (NSN 7540-01-207-5539)	Unclassified Label
SF 711 (NSN 7540-01-207-5541)	Data Descriptor Label

APPENDIX 3. CLASSIFICATION GUIDE

1. PURPOSE. This appendix explains what a classification guide is and describes the information that it must contain in order for it to be used for making derivative classification decisions. Originators of classification guides are encouraged to consult users of guides for input when developing or updating guides. When possible, originators of classification guides are encouraged to communicate within their agencies and with other agencies that are developing guidelines for similar activities to ensure the consistency and uniformly of classification decisions.

2. REQUIREMENT. A classification guide is a document issued by an original classification authority that provides derivative classification instructions. It describes the elements of information that must be protected and the level and duration of classification. In accordance with requirements specified in ISOO Directive Number 1 (32 CFR Part 2001.14), classification guides shall, as a minimum, provide for the following:

a. Identify the subject matter of the classification guide;

b. Identify the original classification authority by name or personal identifier and position;

c. Identify an agency point-of-contact or points-of-contact for questions regarding the classification guide;

d. Provide the date of issuance or last review;

e. State precisely the elements of information to be protected;

f. State which classification level applies to each element of information, and, when useful, specify the elements of information that are unclassified;

g. State, when applicable, special handling caveats;

h. Prescribe declassification instructions or the exemptions category listed in section 1.6(d)(1-8) of Executive Order 12958, the applicable statute, treaty or international agreement; and

i. State a concise reason for classification which, at a minimum, cites the applicable classification category or categories as specified in paragraph 418 of this order.

3. FORMAT. Classification guides shall be unclassified and typically consist of the following components:

a. An unclassified letter of transmittal, cover sheet, or similar document which is used to forward the classification guide to the persons or offices requiring classification guidance. The following information shall be included on or in the classification guide and the transmittal letter as appropriate:

(1) Title and date of the classification guide together with any other information required to identify it specifically.

(2) Reason for the development of the classification guide and the purpose it is intended to serve for the user.

(3) Complete identification and address of the original classification authority responsible for approving the guide.

(4) Conspicuously mark an unclassified transmittal document with the highest classification level of any information transmitted by it. Also mark the transmittal document with an appropriate instruction indicating that it is unclassified when separated from classified enclosures. An example of this statement should read: "Unclassified when separated from classified enclosures".

(5) If the transmittal document itself contains classified information, mark it as required for all other classified information, except:

(a) Conspicuously mark the top and bottom of the transmittal document with the highest classification level of any information contained in the transmittal document or its enclosures; and

(b) mark the transmittal document with an appropriate instruction indicating its overall classification level when separated from its enclosures.

(6) Classification guides shall be disseminated as widely as necessary to ensure the proper and uniform derivative classification of information.

(7) Classification guides shall be reviewed and updated at least once every 5 years.

b. The "classification guide" itself which should be structured as shown in paragraph 4.

4. SAMPLE CLASSIFICATION GUIDE. Figures 1 and 2 which follow illustrate the format for a typical classification guide. This general format can be adapted to specific user needs provided the essential items of information described above are included.

FIGURE #1 - SAMPLE LETTER OF TRANSMITTAL

UNCLASSIFIED

Date:

Subj: Classification Guide Number xx.

From: Associate Administrator for Civil Aviation Security, ACS-1

To: See Distribution

1. Forwarded as attachment to this letter is Classification Guide Number xx, dated January 10, 1999, approved by the Associate Administrator for Civil Aviation Security, ACS-1, as the Original Classification Authority.

2. The guide identifies those information elements and categories associated with Program R&D which are sensitive or national security related and require protection. The guide establishes the appropriate level of classification required and identifies whenever possible the specific timeframe for downgrading or declassifying the information.

3. This guide is to be used by all cleared FAA and contractor personnel associated with Program R&D XXXXX, whose official duties require them to assign derivative classifications.

4. Questions concerning this classification guide and its use should be addressed to ACO-400, Washington, D.C.

(Signature and complete address of the OCA.)

Attachment: Classification Guide Number XX,
dated January 10, 1999

DISTRIBUTION:

(UNCLASSIFIED)

FIGURE #2 - SAMPLE CLASSIFICATION GUIDE

(UNCLASSIFIED)

Title: Classification Guide No. xx
Date of Class. Guide: January 10, 1993
Program: R&D XXXXX
Approval authority: ACS-1, FAA Washington Headquarters, Washington, DC 20591

Subject	Classification Instructions		
	Level	Reason	Duration
1. Program Planning	U	1.5(g)	
2. Threat & Vulnerability Assessment for Specific Facilities	S	1.5(g)	Jan. 10, 2001
3. Technical Scope of Program	S	1.5(g)	Completion of KDP-1 or Jan. 10, 2001 whichever is earlier.
4. Equipment vulnerabilities	U		
5. Communications Security (COMSEC) Interface Requirements	C	1.5(g)	Jan. 10, 2001

(UNCLASSIFIED)

APPENDIX 4. MARKING CLASSIFIED INFORMATION

FIGURE 1. EXAMPLE OF PORTION MARKING

In the sample format shown, the classifier has determined that the information in paragraph 2 shall be protected at the "SECRET" level and has indicated this by portion marking the paragraph with an (S). All other paragraphs are unclassified.

SECRET
(unclassified sample)

SUBJECT:_____ (U)

1. (U) This paragraph contains unclassified information. Therefore, this portion will be marked with the designation "U" in parentheses.

2. (S) This paragraph contains "SECRET" information. Therefore, this portion shall be marked with the designation "S" in parentheses.

3. (U) This paragraph contains no classified information. Therefore, it will also be marked with the designation "U" in parentheses.

SECRET

FIGURE 1

APPENDIX 4. MARKING CLASSIFIED INFORMATION

FIGURE 2. EXAMPLE OF DERIVATIVE CLASSIFICATION

SECRET
(unclassified sample)

SUBJECT:_____(U)

1. (U) This paragraph contains unclassified information.

2. (S) This paragraph contains SECRET information.

3. (U) This paragraph contains unclassified information.

SOURCE DOCUMENT

SECRET

SECRET
(unclassified sample)

SUBJECT:_____(U)

1. (S) This paragraph contains information taken from the second paragraph of the source document and is therefore portion marked with an (S) to show that it contains SECRET information.

2. (U) This paragraph contains unclassified information. Therefore, this portion shall be marked with the designation (U).

DERIVATIVE DOCUMENT

SECRET

APPENDIX 4. MARKING CLASSIFIED INFORMATION

FIGURE 3. PORTION MARKING DOCUMENTS

SECRET
(unclassified sample)

TO: Director
National Security Agency
Fort George G. Meade, Maryland 20755

SUBJECT: Portion Marking (U)

1. (U) This is a sample of a letter with multiple parts. In this sample, paragraph one in its entirety contains SECRET information, but the lines of the opening portion do not. Therefore, this portion shall be marked with the designation "U" in parentheses.

(S) This subparagraph contains information classified SECRET as indicated by the "S" portion marking.

(1) (C) The text in this subparagraph contains information classified CONFIDENTIAL.

(2) (U) This part of the sample document is unclassified.

2. (U) This part contains no classified information.

a. When a paragraph and all its subparagraphs are unclassified, there is no need to portion mark the subparagraphs.

b. This subparagraph is also unclassified.

FOR THE ADMINISTRATOR:

(Official's name and title)

Classified By: FAA/ACS-1
Reason: 1.5(g)
Declassify On: Jan. 10, 2001

FAA Secret Log No: S-xxxxx

SECRET

APPENDIX 4. MARKING CLASSIFIED INFORMATION

FIGURE 4. OVERALL CLASSIFICATION MARKING

SECRET
(unclassified sample)

SUBJECT: Overall Classification Marking (S)

TO: All FAA Personnel

1. (U) The paragraph contains UNCLASSIFIED information.

2. (C) This paragraph contains CONFIDENTIAL information.

3. (S) The overall classification shall be conspicuously marked at the top and bottom.

SECRET

---

1. If the document contains more than one page, place the overall marking at the top and bottom of the outside of the front cover, on the title page, on the first page, and on the outside of the back cover.

2. If a classified publication is without a cover page, show the overall classification on the first page. Mark other internal pages with the highest classification level of information contained on that page; or, when necessary for production efficiency, mark each internal page with the overall classification of the document.

3. The highest classification level of any portion of this document is Secret. Therefore, conspicuously place an overall classification of Secret at the top and bottom of this document.

APPENDIX 4. MARKING CLASSIFIED INFORMATION

FIGURE 5. THE "CLASSIFIED BY" LINE FOR DERIVATIVE CLASSIFICATION

SECRET
(unclassified sample)

Document Title (U)

Federal Aviation Administration
Washington, DC 20591

Classified By: FAA Class Guide No: XXX
dated Jan. 10, 1993
Reason: 1.5 (a) and (d)
Declassify On: Jan. 10, 1998

SECRET

SECRET
(unclassified sample)

back cover

SECRET

APPENDIX 4. MARKING CLASSIFIED DOCUMENTS

FIGURE 6. THE "CLASSIFIED BY" LINE FOR ORIGINAL CLASSIFICATIONS

SECRET
(unclassified sample)

Document Title (U)

Federal Aviation Administration
Washington, DC 20591

Classified By: ACS-1

or

Classified By: FAA/ACS-1
Reason: The original classifier shall identify the reason(s) for the decision to classify.

Declassify On: Apply a date which may not exceed 10 years from of the original decision.

SECRET

APPENDIX 4. MARKING CLASSIFIED INFORMATION

FIGURE 7. THE "DECLASSIFY ON" LINE FOR ORIGINAL CLASSIFICATION

SECRET
(unclassified sample)

1. For originally classified documents: The last essential marking indicates the duration of classification.

2. Whenever possible, link the duration of classification to a specific date or event:

Declassify On: Jan. 10, 1998
or
Declassify On: Completion of 1993 ASEC Conference

3. When the Declassify On by line of the source document is marked Originating Agency's Determination Required or (OADR), mark the derivative document to indicate:

(a) The fact that the source document is marked with this instruction:

and

(b) the date of origin of the source document.

4. This marking will permit the determination of when the classified information is 25 years old and, if permanently valuable, the information will be subject to automatic declassification as specified in paragraph 205 a (1) through (9) of this order.

Declassify On: Source document marked "OADR"
Date of source 10/10/93

In accordance with E.O. 12958, if the source document was marked with this instruction "OADR" and there is no permanent historical value, the document will automatically be declassified within 5 years from the specified date of document.

NOTE: OADR is not an approved marking for documents originally classified under E.O. 12958.

SECRET

APPENDIX 4. MARKING CLASSIFIED INFORMATION

FIGURE 8. THE "DECLASSIFY ON" LINE FOR DERIVATIVE CLASSIFICATION

SECRET
(unclassified sample)

1. For derivatively classified documents: If all classified information is derived from a single source, carry forward the declassification instruction from the source document.

2. If multiple sources are used, specify on the "Derived from" line of the document to indicate that more than one classified source was used.

3. When a document is classified on the basis of more than one source document, the "Derived from" line shall specify Multiple Sources.

4. Maintain the identification of all classified sources with the file or record copy of the document. If practicable, include the list with all copies of the document.

5. The Derived from line shall include: date of source document, agency, where available, and office of origin.

Derived from: Multiple Sources

Source 1: Memo of July 10, 2004
Name and organization of classifier

Source 2: Report of Feb. 2, 2000
Name and organization of classifier

SECRET

APPENDIX 4. MARKING CLASSIFIED INFORMATION

FIGURE 9. DOWNGRADING INSTRUCTIONS

TOP SECRET
(unclassified sample)

Occasionally, the original classifier can predetermine a date or event upon which the decreased sensitivity of the information will permit its downgrading. In this example this TOP SECRET document will automatically be downgraded to SECRET on the date shown.

Downgrade To: SECRET
On: Jan. 10, 1997

TOP SECRET

SECRET
(unclassified sample)

In this example a SECRET document will be downgraded automatically to CONFIDENTIAL upon a specific event.

Downgrade To: CONFIDENTIAL
On: Completion of 1998 ASEC Conference

SECRET

APPENDIX 4. MARKING CLASSIFIED INFORMATION

FIGURE 10. MARKING FOREIGN GOVERNMENT INFORMATION

GEHEIM
(unclassified sample)

DEUTSCHE INDUSTRIE-NORMEN

January 22, 1990

GEHEIM

When the security classification on a foreign government document is already shown in English, apply no other markings to the document. If the document displays the foreign classification as shown above, mark the overall equivalent U.S. classification on the document(s) as shown below.

GEHEIM
SECRET
(unclassified sample)

DEUTSCHE INDUSTRIE-NORMEN
(GERMAN INDUSTRIAL STANDARDS) (U)

January 22, 1998

GERMAN INFORMATION

GEHEIM

APPENDIX 4. MARKING CLASSIFIED INFORMATION

FIGURE 10-1. FOREIGN GOVERNMENT INFORMATION

SECRET
(unclassified sample)

FEDERAL AVIATION ADMINISTRATION
Washington, DC 20591

March 22, 1993

INDUSTRIAL STANDARDS (U)

FOREIGN GOVERNMENT INFORMATION
or
THIS DOCUMENT CONTAINS
GERMAN INFORMATION

Classified By: Multiple Sources
Declassify On: (2003) (provide month or complete date here)

SECRET

Mark FAA documents that contain foreign government information with the marking "FOREIGN GOVERNMENT INFORMATION," or, as shown above, "THIS DOCUMENT CONTAINS (NAME OF COUNTRY) INFORMATION."

In addition, portion mark to identify the foreign government origin, for example "(FRG-C)." See Figure 10-2.

APPENDIX 4. MARKING CLASSIFIED INFORMATION

FIGURE 10-2. FOREIGN GOVERNMENT INFORMATION

SECRET
(unclassified sample)

1. (FRG-S) This sample shows portion markings in a document that contain foreign classified information.
This paragraph would contain GERMAN SECRET information.

2. (FRG-C) The recipient of a foreign classified document is responsible for ensuring that the classification and the country of origin appear in ENGLISH on the document.
This paragraph would contain GERMAN CONFIDENTIAL information.

3. (C) The purpose of the portion markings is to distinguish the foreign information from the U.S. information. This paragraph is marked to show that no foreign classified is contained in it.

SECRET

---

1. Some foreign documents use a fourth classification level designated "Restricted." Apply no other classification to a foreign government document marked RESTRICTED or the foreign equivalent of the word, but add the following notation to the face of the document. "This material is to be safeguarded in accordance with this order."

2. Foreign "Restricted" information contained in a U.S. document requires protection equal to that required for CONFIDENTIAL material. If an otherwise unclassified document contains foreign "Restricted" information, mark the document CONFIDENTIAL and apply portion marking such as "(FRG-R)."

APPENDIX 5. Foreign and International Organization Security Classifications

Country	TOP SECRET	SECRET	CONFIDENTIAL	.....
Albania	TEPER SEKRET	SEKRET	BESNIK SEKRET	ZYRTAK
Argentina	ESTRICTAMENTE SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Australia	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Austria	STRENG GEHEIM	GEHEIM	VERSCHLUSS	
Belgium French	TRES SECRET	SECRET	CONFIDENTIEL	DIFFUSION RESTREINTE
Flemish	ZEER GEHEIM	GEHEIM	VERTROUWELIJK	BEPERKTE VERSPREIDING
Bolivia	SUPERSECRETO or MUY SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Brazil	ULTRA SECRETO	SECRETO	CONFIDENCIAL	RESERVADO (used for "FOR OFFICIAL USE ONLY")
Bulgaria	STROGO SEKRETEN	SEKRETEN TAJNO	POVERITELEN	ZAKRITO PISMO
Cambodia	TRES SECRET	SECRET	SECRET/CONFIDENTIAL	
Canada	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Chile	SECRETO	SECRETO	RESERVADO	RESERVADO
China	绝密	极机密	机密	
Colombia	ULTRA SECRETO	SECRETO	RESERVADO	CONFIDENCIAL RESTRINGIDO
Costa Rica	ALTO SECRETO	SECRETO	CONFIDENCIAL	
Cuba	MUY SECRETO	SECRETO		
Czechoslovakia	PRÍSNĚ TAJNE	TAJNE	DUVERNE OBÝCEJNE	
Denmark	YDERST HEMMELIGT	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG
Ecuador	SECRETISIMO	SECRETO	CONFIDENCIAL	RESERVADO

APPENDIX 5. Foreign and International Organization Security Classifications—Continued

Country	TOP SECRET	SECRET	CONFIDENTIAL	.....
Egypt	SIRRI LILGAYAH سري للغاية	SIRRI JIDDAH سري جدا	SIRRI سري	MAHSUR محصور
El Salvador	ULTRA SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Ethiopia	YEMIAZ BIRTOU MISTIR	MISTIR	KILKIL	
Finland	ERITTAIN SALAINEN	SALAINEN		
France	TRES SECRET	SECRET DEFENSE	CONFIDENTIEL DEFENSE	DIFFUSION RESTREINTE
Germany	STRENG GEHEIM	GEHEIM	VS-VERTRAULICH	
Greece	ΑΚΡΩΣ ΑΠΟΡΡΗΤΟΝ	ΑΠΟΡΡΗΤΟΝ	ΕΜΠΙΣΤΕΥΤΙΚΟΝ	ΠΕΡΙΩΡΙΣΜΕΝΗΣ ΧΡΗΣΕΩΣ
Guatemala	ALTO SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Haiti		SECRET	CONFIDENCIAL	
Honduras	SUPER SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Hong Kong	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Hungary	SZIGORÚAN TITKOS	TITKOS	BIZALMAS	
Iceland	ALGJORTI	TRUNADARMAL		
India	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Indonesia	SANGAT RAHASIA	RAHASIA	TERBATAS	
Iran	BEKOLI SERRI بكلي سري	SERRI سري	KHEILI MAHRAMANEH خيلي محرمانة	MAHRAMANEH محرمانة
Iraq	SIRRI LILGAYAH سري للغاية	SIRRI سري		
Ireland English	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Irish	AN-SICREIDEACH	SICREIDEACH	RUNDA	SRIANTA

APPENDIX 5. Foreign and International Organization Security Classifications—Continued

Country	TOP SECRET	SECRET	CONFIDENTIAL	.....
Israel	SODI BEYOTER סודי ביותר	SODI סודי	SHAMUR שמור	MUGBAL (RESTRICTED) מוגבל
Italy	SEGRETISSIMO	SEGRETO	RISERVATISSIMO	RISERVATO
Japan	KIMITSU 機密	GOKUHI 国密	HI 秘	TORIATSUKAICHUI 取扱注意 BUGAIHI 部外秘
Jordan	SIRRI LILGAYAH سري للغاية	SIRRI سري	MAKTUM مكتوم	MAHDUD محدود
Korea	I KUP PI MIL I	II KUP PI MIL II	III KUP PI MIL III	
Laos	TRES SECRET	SECRET	SECRET/CONFIDENTIEL	DIFFUSION RESTREINTE
Lebanon	TRES SECRET	SECRET	CONFIDENTIEL	
Mexico	ALTO SECRETO	SECRETO	CONFIDENCIAL	RESTRINGIDO ("FOUO" or "LIMITED DISTRIBUTION")
Netherlands	ZEER GEHEIM	GEHEIM	CONFIDENTIEEL or VERTROUWELIJK	DIENSTGEHEIM
New Zealand	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Nicaragua	ALTO SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Norway	STRENGT HEMMELIG	HEMMELIG	KONFIDENSIELL	BEGRENSET
Pakistan	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Paraguay	SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Peru	ESTRICTAMENTE SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Philippines	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED

8|29|97

Foreign and International Organization Security Classifications—Continued

Country	TOP SECRET	SECRET	CONFIDENTIAL	.....
Poland	ŚCIŚCLE TAJNE	TAJNE	POUFNE	DO UZYTKU OFICJALNEGO
Portugal	MUITO SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Romania	STRICT SECRET	SECRET	SECRET DU SERVICIU	SECRET DU SERVICIU
Saudi Arabia	SIRRI LILGAYAH سري للغاية	SIRRI سري		
Spain	MAXIMO SECRETO	SECRETO	CONFIDENCIAL	DIFUSION LIMITADA
Sweden	HEMLIG (two red borders)	HEMLIG (one red border)		
Switzerland	NOTE: TOP SECRET has a distinguish it from SECRET	registration number to and CONFIDENTIAL		
Three languages French	TRES SECRET	SECRET DEFENSE	CONFIDENTIEL DEFENSE	DIFFUSION RESTREINTE
German	STRENG GEHEIM	GEHEIM	VERTRAULICH	
Italian	SEGRETISSIMO	SEGRETO	RISERVATISSIMO	RISERVATO
Syria	SIRRI LILGAYAH سري للغاية	SIRRI سري	MAKTUM مكتوم (NOT CONFIRMED)	MAHDUD محدود
Taiwan	絕對機密	極機密	機密	密
Thailand	LAP THI SUT ลบ ที่สุด	LAP MAK ลับมาก	LAP ลบ	POK PIT ปกปิด
Turkey	ÇOK GİZLİ	GİZLİ	ÖZEL	HIZMETE ÖZEL
Union of South Africa English	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Afrikaans	UITERS GEHEIM	GEHEIM	VERTROULIK	BEPERK

APPENDIX 5. Foreign and International Organization Security Classifications—Continued

Country	TOP SECRET	SECRET	CONFIDENTIAL	.....
United Kingdom	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Uruguay	ULTRA SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Vietnam Vietnamese	TỐI MẬT	MẬT	KÍN	TƯ MẬT
French (Old Usage)	TRES SECRET	SECRET DEFENSE	CONFIDENTIEL DEFENSE	DIFFUSION RESTREINTE
Yugoslovia	STROGO POVERLJIVO	POVERLJIVO		

APPENDIX 5. Foreign and International Organization Security Classifications—Continued

International Organization	TOP SECRET	SECRET	CONFIDENTIAL	
NATO	COSMIC TOP SECRET	NATO SECRET	NATO CONFIDENTIAL	NATO RESTRICTED

"ATOMAL" is an exclusive designation used by NATO to identify "Restricted Data" or "Formerly Restricted Data" information released by the U.S. Government to NATO.

APPENDIX 6. EXTRACTS FROM U.S.C. TITLE 18 AND TITLE 50

SECTION 1. Title 18-Crimes and Criminal Procedures

Section 793. Gathering, transmitting or losing defense information.

(a) Whoever, for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation, goes upon, enters, flies over, or otherwise obtains information concerning any vessel, aircraft, work of defense, navy yard, naval station, submarine base, fueling station, fort, battery, torpedo station, dockyard, canal, railroad, arsenal, camp, factory, mine, telegraph, telephone, wireless, or signal station, building, office, research laboratory or station or other place connected with the national defense owned or constructed, or in progress of construction by the United States or under the control of the United States, or of any of its officers, departments, or agencies, or within the exclusive jurisdiction of the United States, or any place in which any vessel, aircraft, arms, munitions, or other materials or instruments for use in time of war are being made, prepared, repaired, stored, or are the subject of research or development, under any contract or agreement with the United States, or any department or agency thereof, or with any person on behalf of the United States, or otherwise on behalf of the United States, or any prohibited place so designated by the President by proclamation in time of war or in case of national emergency in which anything for the use of the Army, Navy, or Air Force is being prepared or constructed or stored, information as to which prohibited place the President has determined would be prejudicial to the national defense; or

(b) Whoever, for the purpose aforesaid, and with like intent or reason to believe, copies, takes, makes, or obtains, or attempts to copy, take, make, or obtain, any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense; or

(c) Whoever, for the purpose aforesaid, receives or obtains or agrees or attempts to receive or obtain from any person, or from any source whatever, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note, of anything connected with the national defense, knowing or having reason to believe, at the time he receives or obtains, or agrees or attempts to receive or obtain it, that it has been or will be obtained, taken, made, or disposed of by any person contrary to the provisions of this chapter; or

(d) Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the processor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, or transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it; or

(e) Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the processor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it; or

(f) Whoever, being entrusted with or having lawful possession or control of any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, note, or information, relating to the national defense, (1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of this trust, or to be lost, stolen, abstracted, or destroyed, or (2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of its trust, or lost, or stolen, abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior or officer -- Shall be fined not more than $10,000 or imprisoned not more than ten years or both.

(g) If two or more persons conspire to violate any of the foregoing provisions of this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties of such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy.

(h) (1) Any person convicted of a violation of this section an shall forfeit to the United States, irrespective of any provision of State law, any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, from any foreign

government, or any faction or party or military or naval force within a foreign county, whether recognized or unrecognized by the United States, as the result of such violation.

(2) The court, in imposing sentence on a defendant for a conviction of a violation of this section, shall order that the defendant forfeit to the United States all property described in paragraph (1) of this subsection.

Section 794. Gathering or delivering defense information to aid foreign government.

(a) Whoever, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, communicates, delivers, or transmits, or attempts to communicate, deliver, or transmit, to any foreign government, or to any faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States, or to any representative, officer, agent, employee, subject, or citizen thereof, either directly or indirectly, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense, shall be punished by death or by imprisonment for any term of years or for life.

(b) Whoever, in time of war, with intent that the same shall be communicated to the enemy, collects, records, publishes, or communicates, or attempts to elicit any information with respect to the movement, numbers, description, condition, or disposition of any of the Armed Forces, ships, aircraft, or war materials of the United States, or with respect to the plans or conduct, or supposed plans or conduct of any naval or military operations, or with respect to any works or measures undertaken for or connected with, or intended for the fortification or defense of any place, or any other information relating to the public defense, which might be useful to the enemy, shall be punished by death or by imprisonment for any term of years or for life.

(c) If two or more persons conspire to violate this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the defense which is the object of such conspiracy.

(d) (1) Any person convicted of a violation of this section shall forfeit to the United States irrespective of any provision of State law --

(A) any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation, and

(B) any of the person's property used, or intended to be used, in any manner or part, to commit, or to facilitate the commission of, such violation.

(2) The court, in imposing sentence on a defendant for a conviction of a violation of this section, shall order that the defendant forfeit to the United States all property described in paragraph (1) of this subsection.

Section 795. Photographing and sketching defense installations.

(a) Whenever, in the interests of national defense, the President defines certain vital military and naval installations or equipment as requiring protection against the general dissemination of information relative thereto, it shall be unlawful to make any photograph, sketch, picture, drawing, map or graphical representation of such vital military and naval installations or equipment without first obtaining permission of the commanding officer of the military or naval post, camp, or station, or naval vessels, military and naval aircraft, and any separate military or naval command concerned, or higher authority, and promptly submitting the product obtained to such commanding officer or higher authority for censorship or such other action as he may deem necessary.

(b) Whoever violates this section shall be fined not more that $1,000 or imprisoned not more than one year, or both.

Section 796. Use of aircraft for photographing defense installation.

Whoever uses or permits the use of an aircraft or any contrivance used, or designed for navigation or flight in the air, for the purpose of making a photograph, sketch, picture, drawing, map or graphical representation of vital military or naval installations or equipment, in violation of section 795 of this title, shall be fined not more than $1,000 or imprisoned not more than one year, or both.

Section 797. Publication and sale of photographs of defense installations.

On and after thirty days from the date upon which the President defines any vital military or naval installation or equipment as being within the category contemplated under section 795 of this title, whoever reproduces, publishes, sells or gives away any photograph, sketch, picture, drawing, map, or graphical representation of the vital military or naval installations or equipment so defined, without first obtaining permission of the commanding officer of the military or naval post, camp, or station concerned, or higher authority, unless such photograph, sketch, picture, drawing, map, or graphical representation has clearly indicated thereon that it has been censored by the proper military or naval authority, shall be fined not more than $1,000 or imprisoned not more than one year, or both.

Section 798. Disclosure of classified information.

(a) Whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States any classified information --

(1) concerning the nature, preparation, or use of any code, cipher, or cryptographic system of the United States or any foreign government; or

(2) concerning the design, construction, use, maintenance, or repair of any device, apparatus, or appliance used or prepared or planned for use by the United States or any foreign government for cryptographic or communication intelligence purposes; or

(3) concerning the communication intelligence activities of the United States or any foreign government; or

(4) obtained by the processes of communication intelligence from the communications of any foreign government, knowing the same have been obtained by such processes -- Shall be fined not more than $10,000 or imprisoned not more than ten years, or both.

(b) As used in subsection (a) of this section -- the term "classified information" means information which, at the time of a violation of this section, is, for reasons of national security, specifically designated by a United States Government Agency for limited or restricted dissemination or distribution; The terms "code," "cipher," and "cryptographic system" include in their meanings, in addition to their usual meanings, any method of secret writing and any mechanical or electrical device or method used for the purpose of disguising or concealing the contents, significance, or meanings of communications;

The term "foreign government" includes in its meaning any person or persons acting or purporting to act for or on behalf of any faction, party, department, agency, bureau, or military force of or within a foreign country, or for or on behalf of any government or any person or persons purporting to act as a government within a foreign country, whether or not such government is recognized by the United States;

The term "communication intelligence" means all procedures and methods used in the interception of communications and the obtaining of information from such communications by other than the intended recipients;

The term "unauthorized person" means any person who, or agency which, is not authorized to receive information of the categories set forth in subsection (a) of this section, by the President, or by the head of a department or agency of the United States Government which is expressly designated by the President to engage in communication intelligence activities for the United States.

(c) Nothing in this section shall prohibit the furnishing, upon lawful demand, of information to any regularly constituted committee of the Senate or House of Representatives of the United States of America, or joint committee thereof.

Section 1001. Statements or entries generally.

Whoever, in any matter within the jurisdiction of any department or agency of the United States knowingly and willfully falsifies, conceals or covers up by any trick, scheme, or device a material fact, or makes any false, fictitious or fraudulent statements or representations, or makes or uses any false writing or document knowing the same to contain any false, fictitious or fraudulent statement or entry, shall be fined not more than $10,000 or imprisoned not more than five years, or both.

SECTION 2 - TITLE 50 WAR AND NATIONAL DEFENSE

Section 783. Offenses.

(b) Communication of classified information by Government officer or employee.

It shall be unlawful for any officer or employee of the United States or of any department or agency thereof, or of any corporation the stock of which is owned in whole or in major part by the United States or any department or agency thereof, to communicate in any manner or by any means, to any other person whom such officer or employee knows or has reason to believe to be an agent or representative of any foreign government or an officer or member of any Communist organization as defined in paragraph (5) of section 782 of this title, any information of a kind which shall have been classified by the President (or by the head of any such department, agency, or corporation with the approval of the President) as affecting the security of the United States, knowing or having reason to know that such information has been so classified, unless such officer or employee shall have been specifically authorized by the President, or by the head of the department, agency, corporation by which this officer or employee is employed, to make such disclosure of such information.

c. Receipt of, or attempt to receive, by foreign agent or member of Communist organization, classified information.

It shall be unlawful for any agent or representative of any foreign government, or any officer or member of any Communist organization as defined in paragraph (5) to section 782 of this title, knowingly to obtain or receive, or attempt to obtain or receive, directly or indirectly, from any officer or employee of the United States or of any department or agency thereof or of any corporation the stock of which is owned in whole or in major part by the United States or any department or agency thereof, any information of a kind which shall have been classified by the President (or by the head of any such department, agency, or corporation with the approval of the President) as affecting the security of the United States, unless special authorization for such communication shall first have been obtained from the head of the department, agency, or corporation having custody of or control over such information.

(d) Penalties for violation.
Any person who violates any provision of this section shall, upon conviction thereof, be punished by a fine of not more than $10,000, or imprisonment for not more than ten years, or by both such fine and such imprisonment, and shall, moreover, be thereafter ineligible to hold any office, or place of honor, profit, or trust created by the Constitution or laws of the United States.

(e) Limitation period.
Any person may be prosecuted, tried, and punished for any violation of this section at any time within ten years after the commission of such offense, notwithstanding the provisions of any other statute of limitations: Provided, that if at the time of the commission of the offense such person is an officer or employee of the United States or of any department or agency thereof, or of any corporation the stock of which is owned in whole or in major part by the United States or any department or agency thereof, such person may be prosecuted, tried and punished for any violation of this section at any time within ten years after such person has ceased to be employed as such officer or employee.

f. Membership as not violation per se.
Neither the holding of office nor membership in any Communist organization by any person shall constitute per se a violation of subsection (a) or subsection (c) of this section or of any other criminal statute.

<u>Section 797. Security regulations and orders, penalty for violation</u>.

(a) Whoever willfully shall violate any such regulation or order as, pursuant to lawful authority, shall be or has been promulgated or approved by the Secretary of Defense, or by any military commander designated by the Secretary of Defense, or by the Director of the National Advisory Committee for Aeronautics, for the protection or security of military or naval aircraft, airports, airport facilities, vessels, harbors, ports, piers, water-front facilities, bases forts, posts, laboratories, stations, vehicles, equipment, explosives, or other property or places subject to the jurisdiction

administration, or in the custody of the Department of Defense, any Department or agency of which said Department consists, or any officer or employee of said Department or agency, or of the National Advisory Committee for Aeronautics or any officer or employee thereof, relating to fire hazards, fire protection, lighting, machinery, guard service, disrepair, disuse or other unsatisfactory conditions thereon, or the ingress thereto or egress or removal of persons therefrom, or otherwise providing for safeguarding the same against destruction, loss, or injury by accident or by enemy action, sabotage or other subversive actions, shall be guilty of a misdemeanor and upon conviction thereof shall be liable to a fine of not to exceed $5,000 or to imprisonment for not more than one year, or both.

(b) Every such regulation or order shall be posted in conspicuous and appropriate places.

APPENDIX 7. CONSTRUCTION REQUIREMENTS FOR CONTROLLED AREAS

1. GENERAL. This appendix describes the construction requirements for closed areas, vaults, and strongrooms. These requirements are intended to be compatible with the construction requirements specified in the latest edition of Order 1600.6. In the event of conflict between the requirements specified herein and the requirements of any other order or directive, the SSE shall be notified. When the conflict cannot be resolved by the SSE, it will be brought to the attention of ACP-300 through ACO-400.

2. CONSTRUCTION REQUIREMENTS FOR CLOSED AREAS. This paragraph specifies the minimum safeguards and standards required for the construction of closed areas that are approved for use for safeguarding classified material. These criteria and standards apply to all new construction and reconstruction, alterations, modifications, and repairs of existing areas. They will also be used by the SSE and management in evaluating the adequacy of existing areas. Plans and proposals for construction of closed areas shall be coordinated with and approved by the SSE before implementation.

a. Hardware. Only heavy duty builder's hardware shall be used in construction. All screws, nuts, bolts, hasps, clamps, bars, 2-inch square mesh of No. 11-gauge wire (hereinafter referred to as "wire mesh"), 18-gauge expanded metal, hinges, pins, and so on, shall be securely fastened to preclude surreptitious removal and ensure visual evidence of tampering. Hardware accessible from outside the area shall be peened, pinned, brazed, or spotwelded to preclude removal.

b. Walls. Construction of walls may be of plaster, gypsum wallboard, metal panels, hardboard, wood, plywood, glass, wire mesh, expanded metal, or other materials offering resistance to, and evidence of, unauthorized entry into the area. If insert-type panels are used, a method shall be devised to prevent the removal of such panels without leaving visual evidence of tampering. Should any of the outer walls be adjacent to space not controlled by the FAA office or activity, the walls shall be constructed of more substantial building materials, such as brick, concrete, and similar material. If visual access is a factor, area barrier walls up to a height of 8 feet shall be of opaque or translucent construction. If visual access is not a factor, the area barrier walls may be of wire mesh, expanded metal, glass, or other non-opaque material offering similar resistance to, and evidence of, unauthorized entry into the area.

c. Windows. Windows, which open, that are less than 18 feet from an access point (for example, another window outside the area, roof, ledge, or door) shall be fitted with 1/2 inch bars (separated by no more than 6 inches), plus crossbars to prevent spreading, 18-gauge expanded metal, or wire mesh securely fastened on the inside. When visual access is a factor, the windows shall be kept closed and locked at all times, and shall also be made translucent or opaque by any practical method, such as painting or covering the inside of the glass. During nonworking hours, the windows shall be closed and securely fastened to preclude surreptitious removal of classified material.

d. Doors. Doors shall be substantially constructed of wood or metal. When windows, panels, or similar openings are used, they shall be secured with 18-gauge expanded metal or with wire mesh securely fastened on the inside. If visual access is a factor, the windows shall be translucent or opaque. When doors are used in pairs, an astragal (overlapping molding) shall be installed where the doors meet.

e. Door Louvers or Baffle Plates. When used they shall be reinforced with 18-gauge expanded metal or with wire mesh fastened inside the area.

f. Door Locking Devices. Entrance doors shall be secured with either an approved built-in combination lock, an approved combination padlock, or with an approved key-operated padlock. Other doors shall be secured from the inside with a panic bolt (for example, actuated by a panic bar); a dead-bolt, a rigid wood or metal bar, (which shall preclude "springing") which extends across the width of the door and is held in position by solid clamps, preferably on the door casing, or by other means approved by the SSE.

g. Ceilings. Ceilings shall be constructed of plaster, gypsum wall board material, panels, hardboard, wood, plywood, ceiling tile, or other material offering similar resistance to and detection of unauthorized entry. Wire mesh or other non-opaque material offering similar resistance to, and evidence of, unauthorized entry into the area may be used if visual access to classified material is not a factor. When wall barriers do not extend to the slab of the floor above and a false ceiling is created, the false ceiling must be reinforced with wire mesh or 18 gauge expanded metal. When wire mesh or expanded metal is used, it must overlap the adjoining walls and be secured in a manner which precludes removal without leaving evidence of tampering. When wall barriers of an area do extend to the slab of the floor above and a false ceiling is added, there is no need for reinforcement.

h. Ceilings (Unusual Cases). There may be instances where there is a valid justification for not erecting a solid suspended ceiling as part of the area. It may be impractical to use a suspended ceiling because of production methods, such as the use of overhead cranes for the movement of bulky equipment within the area; the air conditioning system may be impeded by the construction of a solid suspended ceiling (for example, AIS centers); or the height of the classified material may make a suspended ceiling impractical. In such cases, special provisions, such as approved motion detection devices, shall be made to ensure that surreptitious entry to the area cannot be obtained by entering the area over the top of the barrier walls. Specific guidance shall be obtained from the SSE for an area of this type.

i. Miscellaneous Openings. Where ducts, pipes, registers, sewers, and tunnels are of such size and shape as to permit unauthorized entry (normally in excess of 96 square inches in area and over 6 inches in its smallest dimension), they shall be secured by 18-gauge expanded metal or wire mesh, or, where more practical, by rigid metal bars at least 1/2 inch in diameter extending across their width, with a maximum space of 6 inches between the bars. The rigid metal bars shall be securely fastened at both ends to preclude removal and shall have crossbars to prevent spreading. When wire mesh,

expanded metal, or rigid metal bars are used, care shall be exercised to ensure that classified material cannot be removed through the openings with the aid of any type of instrument. Care shall be taken to ensure that a barrier placed across any waterway (sewer or tunnel) will not cause clogging or offer obstruction to the free flow of water sewage.

3. CONSTRUCTION REQUIREMENTS FOR VAULTS. Use of vaults for the storage of classified material within the FAA requires the prior approval of the SSE and ACO-400. This paragraph specifies the minimum standards required for the construction of vaults that are to be used for the storage of classified material. These standards apply to all new construction and reconstruction, alterations, modifications, and repairs of existing vaults. They will also be used by the SSE and management for evaluating the adequacy of existing vaults. In addition to the requirements given below, the wall, floor, and roof construction shall be in accordance with nationally recognized standards of structural practice. For the vaults described below, the concrete shall be poured in place, and will have a minimum 28-day compressive strength of 2,500 pounds per square inch.

a. Class A Vault.

(1) Floor and Walls. The thickness of the floor and walls shall be determined by structural requirements, but may not be less than 8-inch-thick reinforced concrete. Walls are to extend to the underside of the slab of the floor above.

(2) Roof/Ceiling. The roof or ceiling must be a monolithic reinforced concrete slab of a thickness to be determined by structural requirements, but not less thick than the walls and floors.

(3) Vault Door and Frame Unit. An approved vault door and frame unit shall be used.

(4) Miscellaneous Openings. Omission of all miscellaneous openings is desirable, but not mandatory. Openings of such size and shape as to permit unauthorized entry, (normally in excess of 96 square inches in area and over 6 inches in its smallest dimension) and openings for ducts, pipes, registers, sewers, and tunnels shall be equipped with man-safe barriers such as wire mesh, 18-gauge expanded metal, or rigid metal bars of at least 1/2 inch in diameter extending across their width with a maximum space of 6 inches between the bars. The rigid metal bars shall be securely fastened at both ends to preclude removal and shall have crossbars to prevent spreading. Where wire mesh, expanded metal, or rigid metal bars are used, care shall be exercised to ensure that classified material within the vault cannot be removed with the aid of any type of instrument. Pipes and conduits entering the vault shall enter through walls that are not common to the vault and the structure housing the vault. Preferably such pipes and conduits should be installed when the vault is constructed. If this is not practical, they shall be carried through snug-fitting pipe sleeves cast in the concrete. After installation, the annular space between the sleeve and the pipe of conduit shall be caulked solid with lead, wood, waterproof (silicone) caulking, or similar material, which will give evidence of surreptitious removal.

b. Class B Vault.

(1) Floor. The floor must be a monolithic concrete construction of the thickness of adjacent concrete floor construction, but not less than 4 inches thick.

(2) Walls. The walls must be not less than 8-inch-thick brick, concrete block, or other masonry units. Hollow masonry units shall be the vertical cell type (load bearing) filled with concrete and steel-reinforcing bars. Monolithic steel-reinforced concrete walls at least 4 inches thick may also be used, and shall be used in seismic areas. Walls are to extend to the underside of the roof slab above.

(3) Roof/Ceiling. The roof or ceiling must be a monolithic reinforced concrete slab of thickness to be determined by structural requirements.

(4) Vault Door and Frame Unit. An approved vault door and frame unit shall be used.

(5) Miscellaneous Openings. Omission of all miscellaneous openings is desirable, but not mandatory. Openings of such size and shape as to permit unauthorized entry (normally in excess of 96 square inches in area and over 6 inches in its smallest dimension) and openings for ducts, pipes, registers, sewers, and tunnels shall be equipped with man-safe barriers such as wire mesh, 18-gauge expanded metal, or rigid metal bars of at least 1/2 inch in diameter extending across their width with a maximum space of 6 inches between the bars. The rigid metal bars shall be securely fastened at both ends to preclude removal and shall have crossbars to prevent spreading. Where wire mesh, expanded metal, or rigid metal bars are used, care shall be exercised to ensure that classified material within the vault cannot be removed with the aid of any type of instrument. Pipes and conduits entering the vault shall enter through walls that are not common to the vault and the structure housing the vault. Preferably such pipes and conduits should be installed when the vault is constructed. If this is not practical, they shall be carried through snug-fitting pipe sleeves cast in the concrete. After installation, the annular space between the sleeve and the pipe or conduit shall be caulked solid with lead, wood, waterproof (silicone) caulking, or similar material, which will give evidence of surreptitious removal.

c. Class C Vault.

(1) Floor. Same as for a Class B vault.

(2) Walls. Walls must be not less than 8-inch-thick hollow clay tile (vertical cell double shells) or concrete blocks (thick shells). Monolithic steel-reinforced concrete walls at least 4 inches thick may also be used. Where hollow clay tiles are used and such masonry units are flush, or in contact with, facility exterior walls, they shall be filled with concrete and steel-reinforcing bars. Walls are to extend to the underside of the slab of the floor above.

(3) Roof/Ceiling. Same as for a Class B vault.

(4) Vault Door and Frame Unit. Same as for a Class B vault.

(5) Miscellaneous Openings. Same as for a Class B vault.

4. CONSTRUCTION REQUIREMENTS FOR STRONGROOMS. Use of a strongroom for storage of classified material requires the prior approval of the SSE and ACO-400. This paragraph specifies the minimum standards required for the construction of approved strong rooms for use as storage facilities for classified material.

a. Hardware. Heavy-duty builder's hardware shall be used in construction. All screws, nuts, bolts, hasps, clamps, bars, wire mesh, 18-gauge expanded metal, hinges, pins, and the like shall be securely fastened to preclude surreptitious entry and ensure visual evidence of tampering. Hardware accessible from outside the area shall be peened, brazed, or spot-welded to preclude removal.

b. Walls and Ceilings. Construction shall be of plaster, gypsum board, metal, hardboard, wood, plywood, or other solid, opaque materials offering resistance to and evidence of unauthorized entry into the area. Insert-type panels shall not be used. Should any of the outer walls be adjacent to space not controlled by the FAA office or activity, the walls shall be constructed of more substantial building materials, such as brick, concrete, and similar material.

c. Floors. Floors shall be of solid construction, utilizing materials such as concrete, ceramic tile, and wood.

d. Windows. Windows which open, that are less than 18 feet from an access point (such as another window outside the area, roof, ledge, or door) shall be fitted with 1/2 inch bars (separated by no more than 6 inches), plus crossbars to prevent spreading, 18-gauge expanded metal, or wire mesh securely fastened on the inside to preclude surreptitious removal. In addition to being kept closed at all times, the window shall be translucent or opaqued by any practical method, such as painting or covering the inside of the window.

e. Miscellaneous Openings. Openings for pipes, ducts, registers, sewers, and tunnels of such size and shape as to permit unauthorized entry (normally in excess of 96 square inches in area and over 6 inches in its smallest dimension) shall be equipped with man-safe barriers such as wire mesh, 18-gauge expanded metal, or rigid metal bars of at least 1/2 inch in diameter extending across their width with a maximum space of 6 inches between the bars. The rigid metal bars shall be securely fastened at both ends to preclude removal and shall have crossbars to prevent spreading. Where wire mesh, expanded metal, or rigid metal bars are used, care shall be exercised to ensure that classified material within the room cannot be removed with the aid of any type of instrument.

f. Doors. Doors shall be substantially constructed of wood or metal. When windows, panels, or similar openings are used, they shall be secured with 18 gauge expanded metal or wire mesh securely fastened on the inside. The windows shall be translucent or opaque. When doors are used in pairs, an astragal (overlapping molding) shall be installed where the doors meet.

g. Door Louvers and Baffle Plates. When used they shall be reinforced with wire mesh fastened inside the room.

h. Door Locking Devices. Entrance doors shall be secured by either an approved built-in combination lock or an approved combination padlock, which is secured to the door by a solid metal hasp. Other (non-entry) doors shall be secured from the inside with a panic bolt (for example, activated by a panic bar); a dead bolt; a rigid wood or metal bar, which shall preclude "springing," that extends across the width of the door and is held in position by solid clamps, preferably on the door casing; or by any other means approved by the SSE.

APPENDIX 8. SAMPLE COURIER LETTER

(Date):

SUBJECT: Authority to hand-carry classified information

EXPIRATION DATE: _____
(up to 1 year from date above)

ISSUING OFFICE: (FAA HQ, Region/Center or CASD)
(Official mailing address)

TO: Whom it may concern

1. General: In accordance with Order 1600.2, the following individual is authorized to hand-carry classified information.

a. Name of courier:
b. Grade:
c. Social Security Number:
d. Date/place of birth:
e. Physical characteristics:

(1) Sex:
(2) Height:
(3) Weight:
(4) Hair Color:
(5) Eye Color:

f. Identification card number/type:

g. Security clearance:

h. Employing activity:

2. Description of classified material:

(This should be a concise physical description of the material in the possession of the courier. An example would be:

One - 8- by 11- inch sealed packaged addressed to the
Department of Energy, Office XYZ, Washington, DC, from
FAA Office of Civil Aviation Security,
ACP-300, 800 Independence Ave, S.W.,
Washington, DC. 20591

3. Certification. The undersigned certifies that the courier is familiar with Order 1600.2 and has been briefed regarding his/her courier responsibilities.

4. Authentication. Confirmation of the validity of this letter may be obtained from the undersigned official at telephone number
_____.

(Signature and Title,
Manager, Servicing
Security Element, or
Activity/Office)

APPENDIX 9. CLASSIFIED MATERIAL COURIER INSTRUCTIONS

1. PURPOSE. To establish standard procedures for FAA personnel appointed as couriers of classified material in accordance with provisions of chapter 11.

2. SCOPE. These procedures pertain to national security information. Procedures for Sensitive Compartmented Information, Communication Security (COMSEC), and other information with special handling instructions are contained in security policy regulations pertaining to those programs.

3. APPLICABILITY. These procedures apply to all FAA employees appointed as couriers for classified material. Servicing security elements should provide specific guidance.

4. PROCEDURES.

a. The courier and/or escort shall be cleared for the highest level of classified information carried. The courier shall have one of the following forms of identification in his/her possession:

(1) A valid Armed Forces Identification Card; or

(2) FAA identification card/credential or approved FAA ID media.

b. The courier shall have an original letter issued in accordance with Order 1600.2.

c. COMSEC material will be transported in accordance with the latest edition of Order 1600.8.

d. The courier or escort will be briefed by their servicing security element or Classified Information Account Custodian. The briefing will include the following:

(1) CLASSIFIED MATERIAL WILL REMAIN IN THE PHYSICAL POSSESSION OF THE COURIER AT ALL TIMES DURING TRANSPORT. It shall never be left unattended.

(2) Classified material will only be released to the authorized, designated recipient.

(3) Classified material will not be displayed in public.

(4) Classified material will be transported by the most direct route and intermediate stops will be avoided.

(5) If a vehicle breaks down, the courier will:

(a) Keep the classified material in his/her possession while getting assistance, if traveling unescorted.

(b) If traveling with an escort, the courier will keep possession of the classified material and stay with the vehicle, while the escort shall be sent to obtain assistance.

(c) Advise the SSE as quickly as possible of any possible loss or compromise of classified material or delay in delivery.

(6) Couriers will not use intoxicants while assigned to safeguard classified material.

5. RESPONSIBILITY.

a. The SSE is responsible for ensuring that procedures to designate and brief couriers are implemented appropriately.

b. FAA employees designated as couriers shall be familiar with the provisions of Order 1600.2 regarding packaging, safeguarding, and transportation of classified material.

c. The courier will be held responsible for safeguarding, control, and accountability of the classified material and for immediately reporting to the SSE any circumstances resulting in the loss or possible compromise of the material.

d. The courier is responsible for contacting the SSE if any clarification of these duties is required prior to accepting custody of classified material.

APPENDIX 10. REQUIREMENTS FOR SAFEGUARDING SENSITIVE BUT UNCLASSIFIED INFORMATION

1. The "For Official Use Only" (FOUO) marking is assigned to information at the time of its creation in the FAA or other agency. It is not authorized as a substitute for a security classification marking but is used on official Government information that may be withheld from the public under exemptions 2 through 9 of the Freedom of Information Act which are listed below. Use of the FOUO marking does not mean that the information cannot be released to the public, only that it must be reviewed by the Government prior to its release to determine whether a significant and legitimate Government purpose is served by withholding the information or portions of it.

a. An unclassified document containing FOUO information shall be marked "For Official Use Only" at the bottom of the front cover (if any), on the first page, on each page containing FOUO information, on the back page, and on the outside of the back cover (if any). No portion markings shall be shown.

b. Within a classified document, an individual page that contains both FOUO and classified information shall be marked at the top and bottom with the highest security classification of information appearing on the page. If an individual portion contains FOUO information but no classified information, the portion will be marked "FOUO."

c. FOUO material may be destroyed by tearing into small pieces and assimilating with other waste material. In instances of volume or unusual sensitivity, the material shall be destroyed by shredding, burning, or pulping.

d. Any "For Official Use Only" information released by the FAA to a contractor shall be marked with the following statement prior to transfer:

This document contains information
EXEMPT FROM MANDATORY DISCLOSURE
under the FOIA. Exemptions___apply.

2. <u>FREEDOM OF INFORMATION ACT (FOIA) EXEMPTIONS</u>. This subpart implements sections 552(b) of Title 5, United States Code, which exempts certain records from the public disclosure requirements of section 552(a).

a. <u>Exemption 1 refers to information which is currently and properly classified and is authorized to remain classified in the interest of national security</u>. In accordance with Section 7.63, <u>Records relating solely to matters that are required by Executive Order to be kept secret</u>. Records relating to matters that are specifically authorized to be kept secret in the interest of national defense or foreign policy shall be exempt from public disclosure.

b. Exemption 2 refers to information containing or constituting rules, regulations, orders, manuals, directives, and instructions relating to the internal personnel rules or practice of the agency if performance of a significant function of the agency does not impose requirements directly on the general public.

Section 7.65(a). Records related solely to internal personnel rules and practices. Records related solely to internal personnel rules and practices that are within the statutory exemption include memoranda pertaining to personnel matters, such as staffing policies and policies and procedures for the hiring, training, promotion, demotion, and discharge of employees, and management plans, records, or proposals involving labor-management relationships

c. Exemption 3 refers to information which is specifically exempted from disclosure by statute that permits no discretion on the issue, or in accordance with criteria established by the statute for withholding or referring to the particular types of information to be withheld.

Section 7.67. Records exempted from disclosure by statute. Records relating to matters that are specifically exempted from disclosure by statute (other that section 552(b) of Title 5, United States Code).

d. Exemption 4 refers to trade secrets or commercial or financial information. Records falling under this exemption must contain trade secrets or commercial or financial records, the disclosure of which is likely to cause substantial harm to the competitive position of the source providing the information; impair the Government's ability to obtain necessary information in the future; or impair some other legitimate Government interest.

Section 7.69. Trade secrets and commercial or financial information obtained from a person and privileged or confidential. Trade secrets and commercial or financial information obtained from a person and privileged or confidential are within this statutory exemption.

e. Exemption 5 refers to internal advice recommendations, and subjective evaluations, as contrasted with factual matters, that are reflected in records pertaining to the decisionmaking process of an agency, whether within or among agencies or within or among an agency and its components.

Section 7.71(a). Intragovernmental exchanges. Any record prepared by a Government officer or employee (including those prepared by a consultant or advisory body) for internal Government use is within the statutory exemption to the extent it contains:

(1) Opinions, advice, deliberations, or recommendations.

(2) Confidential communications between a Government attorney or an attorney acting on behalf of the Government which relates to a legal matter.

(3) Information prepared by a Government attorney or an attorney acting on behalf of the Government in anticipation of litigation.

(4) Confidential commercial information generated by the Government where disclosure of such information would prejudice the bargaining position in commercial transactions.

Section 7.71(b). The purpose of this section is to protect internal records that are not routinely available by law to another party in litigation with the Government.

f. Exemption 6 refers to information in personnel and medical files, as well as similar personal information in other files, that if disclosed to the requester would result in a clearly unwarranted invasion of personal privacy.

Section 7.73(a). Protection of personal privacy. Any of the following personnel, medical, or similar records are within the statutory exemption if disclosure would result in a clearly unwarranted invasion of personal privacy.

(1) Personnel and background records.

(2) Medical histories and records concerning individuals.

(3) Any other detailed record containing personal information identifiable with a particular person.

(b). The purpose of this section is to provide a proper balance between the protection of personal privacy and the preservation of the public's right to Department information.

g. Exemption 7 refers to investigative records compiled for the purpose of enforcing civil, criminal, or military law.

Section 7.75(a). Files compiled for law enforcement purposes by the Department or any other Federal, State, or local agency, including those files compiled for the enforcement of regulations, are within the statutory exemption to the extent that production of such records or information could reasonably be expected to interfere with enforcement proceedings.

Section 7.75(b). The purpose of this section is to protect law enforcement files from premature disclosure.

h. Exemption 8 refers to information contained in or related to examination, operation, or condition reports prepared by or on behalf of or for the use of any agency responsible for the regulation or supervision of financial institutions.

Section 7.77. Reports of financial institutions. Any material contained in or related to any examination, operating, or condition report prepared by or on behalf of or for the use of an agency responsible for the regulation or supervision of financial institutions is within the statutory exemption.

i. Exemption 9 refers to geological and geophysical information and data (including maps) concerning wells.

Section 7.79. Geological and geophysical information. Any geological or geophysical information and data (including maps) concerning wells is within the statutory exemption.

3. INFORMATION DESIGNATED AS "LIMITED OFFICIAL USE" (LOU). The Department of State (DOS) policy permits marking documents which do not meet the criteria for classification under E.O. 12958, but nonetheless may have internal sensitivity, with the designation LOU. LOU is not an authorized form or designation of classification to protect national security classified information. LOU Information may include, among other things, information received through privileged sources and certain personnel, medical, investigative, commercial, and financial records and material protected by the Privacy Act. While the designation of information as LOU by FAA personnel is not authorized, FAA offices and activities may receive communications and documents from the DOS or other U.S. foreign affairs agencies that are marked LOU and, for that reason, it is necessary that FAA personnel follow the handling procedures as specified below under paragraphs 4 through 6.

4. INFORMATION DESIGNATED AS "SENSITIVE BUT UNCLASSIFIED INFORMATION" (SBU). The Department of State (DOS) has terminated the use of the handling instruction Limited Official Use (LOU) and has implemented the use of SBU information. Information previously marked as LOU does not have to be remarked as SBU. Employees are not required to mark the information but the document should carry a distribution restriction to make the recipient aware of specific controls. SBU describes information which warrants a degree of protection and administrative control that meets the criteria under Sections 552 and 552a of Title 5, United States Code: Freedom of Information Act, the Privacy Act, and the Computer Security Act of 1987, or Public Law 100-235.

a. SBU information includes, but is not limited to:

(1) Medical, personnel, financial, investigatory, visa, law enforcement, or other

information which, if released, could result in harm or unfair treatment to any individual or group, or could have a negative impact upon foreign policy or relations; and

(2) Information offered under conditions of confidentiality which arises in the course of a deliberative process (or a civil discovery process), including attorney-client privilege or work product, and information arising from the advice and counsel of subordinates to policy matters.

b. Previous regulations regarding LOU material are superseded and LOU becomes SBU effective immediately.

5. ACCESS, DISSEMINATION, AND RELEASE OF SBU INFORMATION. FAA supervisors and employees are responsible for protecting, controlling, disseminating, releasing, and allowing access to SBU material. Employees will limit access to protect SBU information from unintended public disclosure.

a. Employees may circulate SBU material to others, including Foreign Service nationals, to carry out an official United States Government function if not otherwise prohibited by law, regulation, or interagency agreement.

b. SBU information is not required to be marked, but should carry a distribution restriction to make the recipient aware of specific controls. Protection of SBU information stored or processed on automated information systems is also subject to the protective criteria as specified in this order.

c. Regardless of method, transmission of SBU information should be effected through means which limit the potential for unauthorized public disclosure. Information transmitted over unencrypted electronic links such as telephones may be intercepted by unintended recipients, and custodians of SBU information should decide whether specific information warrants a higher level of protection by using a secure fax, secured telephone such as a STU-III, or other encrypted means of communication.

d. FAA personnel must transmit/transport all sensitive information in a manner which limits the potential for unauthorized public disclosure. Employees may send SBU information via the U.S Postal Service, APO, commercial messenger, or unclassified registered pouch provided it is enclosed in an envelope which does not disclose its contents or the fact that it is SBU.

6. HANDLING, TRANSMISSION, MAILING, STORAGE, AND DESTRUCTION OF SBU INFORMATION.

a. FAA employees must handle sensitive information through means which limit the potential for unauthorized public disclosure.

b. During non- and normal working hours, employees shall ensure that SBU information and records are inaccessible to unauthorized personnel and SBU information shall be secure within a locked office or a locked container.

c. Unauthorized disclosure of SBU of information does not constitute a security infraction. However, unauthorized disclosure of SBU information that is protected by the Privacy Act under Title 18 U.S.C. Section 641 may result in criminal and/or civil sanctions against responsible persons.

d. Destruction of SBU documents shall consist of shredding, pulping, or burning.

e. FAA personnel in possession of SBU material are authorized to convey such material to Foreign Government officials and other U.S. Federal, state, and local government departments and agencies as needed to comply with official disclosure policy in the interest of the FAA.

14 C.F.R. PART 191. WITHHOLDING SECURITY INFORMATION FROM DISCLOSURE UNDER THE AIR TRANSPORTATION SECURITY ACT OF 1974.

7. SECTION 191.1 APPLICABILITY.

(a) This part implements section 316(d)(2) of the Federal Aviation Act of 1958 (49 USC 1357(d)(2)) and governs the release of any record, and any information contained therein, in the possession of the FAA which has been obtained or developed in the conduct of research and development activities to develop, modify, test, and evaluate systems, procedures, facilities, and devices to protect persons and property aboard aircraft in air transportation against acts of criminal violence and aircraft piracy.

(b) For the purposes of this part, "record" includes any writing, drawing, map, recording, tape, film, photograph, or other documentary material by which information is preserved.

8. SECTION 191.3. RECORDS AND INFORMATION WITHHELD.

(a) Notwithstanding 5 USC 552, the records described in Section 191.1(a) are not made available for public inspection or copying nor is any information contained in those records released to the public when disclosure thereof is prohibited by the Associate Administrator for Civil Aviation Security (ACS-1) or designee.

(b) Records subject to paragraph (a) of this section include, but are not limited to, those containing information which pertains to:

(1) Any hijacker profile.

(2) Any profile used in baggage screening.

(3) The security program of any airport.

(4) The security program of any air carrier.

(5) Any device for the detection of any explosive or incendiary device or weapon.

(6) Any device for protection against, or detection of, cargo theft.

(7) Any contingency security plan.

(8) Any security communications equipment and procedures.

(9) Any threat of sabotage, terrorism, or air privacy.

(10) The security program of any indirect air carrier and that portion of the security program of the United States Postal Service that relates to security of parcel mail to be transported by air.

9. SECTION 191.5. WHEN DISCLOSURE OF INFORMATION IS PROHIBITED. ACS-1 or designee prohibits disclosure of a record and information contained therein under Section 191.3 if in his/her opinion it would:

(a) Constitute an unwarranted invasion of personal privacy (including, but not limited to, information contained in any personnel, medical, or similar file);

(b) Reveal trade secrets or privileged or confidential commercial or financial information obtained from any person; or

(c) Be detrimental to the safety of persons traveling in air transportation or intrastate air transportation.

10. SECTION 191.7. RECORDS CONTAINING BOTH AVAILABLE AND UNAVAILABLE INFORMATION. If a record contains information that ACS-1 or designee determines cannot be disclosed under this part, but also contains information that can be disclosed, the latter information will be provided for public inspection and copying.