U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION
National Policy

ORDER
1600.2E

Effective Date:
Mar. 13, 2006

SUBJ: Safeguarding Classified National Security Information

National security information concerns the national defense or foreign relations of the United States. We safeguard it to protect our citizens, the national defense, homeland security, and relations with foreign nations.

Executive Order (EO) 12958, Classified National Security Information, as amended by EO 13292, prescribes the system for classifying, safeguarding, and declassifying national security information. Title 32 Code of Federal Regulations (CFR) Parts 2001 through 2004 and Department of Transportation (DOT) Order 1640.4 complement EO 12958.

This order fulfills our duties under EO 12958, Title 32 CFR Parts 2001 through 2004, and DOT Order 1640.4.

Marion C. Blakey
Administrator
Federal Aviation Administration

Distribution: A-WXYZE; A-FOF-0(LTD)

Initiated by: ASH-1

TABLE OF CONTENTS

Chapter 1: GENERAL INFORMATION

1. Purpose of This Order. This order sets up the FAA's program for classifying, declassifying, and safeguarding classified national security information and materials under:

a. Executive Orders (EO):

(1) EO 12958, as amended by EO 13292, Classified National Security Information;

(2) EO 12968, Access to Classified Information; and

(3) EO 12829, The National Industrial Security Program (NISP).

b. Code of Federal Regulations (CFR):

(1) Title, 32, CFR Parts 2001 and 2004, Classified National Security (Directive No. 1);

(2) Title, 32, CFR Part 2002, General Guideline for Systematic Declassification Review of Foreign Government Information;

(3) Title, 32 ,CFR Part 2003, National Security Information -- Standard Forms; and

(4) Title, 49, CFR Part 8, Classified Information: Classification/Declassification/Access.

c. DOT Order 1640.4, Classified Information Management.

The terms "classified national security information" and "classified information" are interchangeable.

2. Who This Order Affects. If you have access to classified information or if you manage operations that use classified information, this order applies to you.

3. Cancellation. FAA Order 1600.2D, Safeguarding Controls and Procedures for Classified National Security Information and Sensitive Unclassified Information of August 29, 1997.

4. Explanation of Policy Changes: This order:

a. Changes its title from "Safeguarding Controls and Procedures for Classified National Security Information and Sensitive Unclassified Information" to "Safeguarding Classified National Security Information."

b. Deletes policy and procedures for protecting sensitive unclassified information (SUI). FAA Order 1600.75 addresses these policies and procedures.

c. Revises responsibilities to conform to EO 12958, as amended. (Chapter 2)

d. Appoints the Assistant Administrator for Security and Hazardous Material, ASH-1 as the FAA's Senior Agency Official (SAO). (Page 2-1, paragraph 4)

e. Renames the title of National Security Information Program Manager to Classified Information Security Program Manager and updates this manager's responsibilities. (Page 2-4, paragraph 7)

f. Assigns duties and responsibilities for Classified Information Security Managers (CISM) and sets up training standards for CISMs. (Page 2-5, paragraph 8 and page 6-3, paragraph 4b(3))

g. Updates responsibilities of Classified Information Account Custodians. (Page 10-3, paragraph 5)

h. Assigns responsibilities and sets policies for National Security Systems (NSS). (Page 2-5, paragraph 8)

i. Addresses training for original classification authorities. (Page 6-2, paragraph 4b)

j. Updates the categories of classified information which include:

(1) Scientific, technological, or economic matters about national security, which includes defense against transnational terrorism;

(2) Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services about national security, which includes defense against transnational terrorism; and

(3) Weapons of mass destruction. (Page 3-1, paragraph 1a(3))

m. Changes declassification instructions and updated policies for automatic, systematic, and mandatory declassification and declassification databases. (Chapters 3, 4, and 7)

n. Adds policies and procedures for emergency access to classified information by individuals who are otherwise not eligible for access. (Page 9-2, paragraph 2m)

o. Adds standards for training on:

(1) Safeguarding classified information; and

(2) Criminal, civil and administrative sanctions for individuals, who fail to protect classified information from unauthorized disclosure. (Chapter 6)

p. Revises procedures and forms for classified material accountability. (Chapter 10)

q. Revises forms the (FAA, we, us) use to administer classified information. (Appendix B)

5. Classified Information Security Policy.

a. FAA employees are personally and individually responsible for proper protection of classified information under their custody and control.

b. FAA managers have specific, nondelegable responsibility for the quality of carrying out this order within their areas of responsibility.

c. By EO 12958 management of classified information will be a critical element or item for performance ratings of:

(1) Original classification authorities;

(2) Classified Information Security Managers; and

(3) All others whose duties significantly involve creating or handling classified information.

d. The FAA classifies information only when necessary for national security, and declassifies it as soon as consistent with the needs of national security.

e. An employee may have access to classified information when:

(1) The Personnel Security Division, AIN-400, or Regional Servicing Security Elements make a favorable determination (security clearance) of eligibility for access;

(2) The employee signs a Standard Form (SF) -312 Classified Information Nondisclosure Agreement; and

(3) The employee has a need-to-know the information.

f. Employees will not remove classified information from FAA facilities without proper authorization. Chapter 9, paragraph 10, discusses methods for removing classified information from FAA facilities.

g. Employees will not disclose classified information originated by another agency without the consent of the originating agency.

h. Employees will keep classified information only when they need it for effective and efficient operation of the FAA or to comply with law or regulation.

i. Managers and employees must preserve and dispose of classified information, documents, and materials that make up permanently valuable records of the Government. (FAA Orders 1350.14 and 1350.15)

j. Department of Defense Manual 5220.22-M, The National Industrial Security Program Operating Manual, prescribes requirements for classified information in FAA contracts, grants, and licensees. (FAA Order 1600.72)

k. National Security Systems (NSS) are automated information systems, including networks and telecommunications that collect, create, communicate, compute, disseminate, process, or store classified information. Our NSS must have controls that:

(1) Prevent access by unauthorized people; and

(2) Ensure integrity of the information.

6. Sensitive Compartmented Information (SCI).

a. Except where specifically mentioned, this order does not address SCI. SCI is a special category of classified information about or drawn from intelligence sources, methods, or analytical processes. The Director of Central Intelligence (DCI) sets up policy and procedures for controlling SCI.

b. The National Security Coordination Division, AEO-300, and the Special Security Officer (SSO) within the division:

(1) Receives and controls SCI for the FAA and oversees all FAA SCI handling and SCI facilities (SCIFs) to ensure they comply with DCI directives, and

(2) Works with customer lines of business (LOB) concerning SCI requirements, operational use of SCI information, and verification of SCI accesses.

c. The Personnel Security Division (AIN-400) processes all requests for background investigations and security clearances and initiates requests to DCI for SCI access authorization. AIN-400 closely coordinates such requests with the AEO SSO, who on approval of an individual for SCI access, will arrange or conduct appropriate security indoctrination for the individual. (FAA Order 1600.1 and SCI Program Order, when published)

Chapter 2: RESPONSIBILITIES

1. Overview. Each person, who has access to classified information or who manages operations that create, use, or handle classified information, has responsibilities under this order.

2. Individual Responsibilities. If you have access to classified information, you must:

a. Protect it from unauthorized disclosure. This means taking the measures of this order to prevent its loss, compromise, or unauthorized disclosure, distribution, or duplication;

b. Safeguard it. This means storing it in a GSA approved security container or approved open storage facility or putting it under the personal observation and control of an authorized person; and

c. Protect it from unauthorized people**.** This means ensuring that unauthorized people do not have exposure, access, or possession of classified information.

3. The Administrator. By EO 12958 heads of agencies that originate or handle classified information must:

a. Display personal commitment and commit senior management to the successful implementation of the program set up under EO 12958;

b. Commit necessary resources to effectively implement EO 12958;

c. Ensure the FAA designs and maintains records systems to:

(1) Safeguard classified information, and

(2) Promote its declassification under the terms of EO 12958 when it no longer meets the standards for continued classification; and

d. Name a Senior Agency Official (SAO) to oversee and manage the program for classifying, declassifying, disclosing, handling, and safeguarding classified information.

4. Senior Agency Official. The Assistant Administrator for Security and Hazardous Materials (ASH-1). ASH-1 is the FAA's SAO, whose responsibilities include:

a. Overseeing the FAA's program for classifying, declassifying, disclosing, handling, destroying, distributing, and safeguarding classified information;

b. Serving as the FAA's principal declassification authority for information originally classified by the FAA and for issuing declassification guidance;

c. Issuing and managing FAA classification and declassification guides.

d. Setting up and managing a classification and declassification database for information originally classified or declassified by the FAA;

e. Issuing guidance which do not change FAA policy, delegation of authority, assignment of responsibility, or have a significant resource impact;

f. Setting up and maintaining security awareness and education programs to support this order;

g. Setting up and managing a continuing inspection program, that includes periodic review and assessment of the FAA's classified products to ensure we properly classify information;

h. Coordinating policies and procedures for safeguarding classified information with other lines of business, offices, and external agencies;

i. Setting up procedures to prevent unnecessary access to classified information including procedures to:

(1) Limit access to cleared personnel;

(2) Show a need for access to classified information before starting administrative security clearance procedures; and

(3) Limit the number of people granted access to classified information consistent with operational needs.

j. Developing plans for safeguarding classified information used in or near hostile or potentially hostile areas;

k. Delegating responsibilities for agency-wide program management to a Classified Information Security Program Manager (CISPM), who manages day-to-day program matters;

l. Taking proper and prompt corrective action when a violation or infraction of EO 12958 and this order occurs;

m. Informing the DOT SAO whenever unauthorized access, loss, or compromise of classified information occurs;

n. Ensuring employee performance ratings include managing classified information as a critical element or item in the ratings of

(1) Classified Information Security Managers, and

(2) All whose duties significantly involve creating or handling classified information;

o. Reporting FAA statistics and costs for protecting classified information to the DOT Director of Security, M-40; and

p. Ensuring prompt and accurate response to any question, appeal, challenge, complaint, or suggestion arising from this order.

5. Management. All levels of management - whose operations use, handle or process classified information - must:

a. Show personal commitment and commit their senior managers to the successful implementation of this order;

b. Effectively manage the classified information under their control;

c. Commit necessary resources to safeguard classified information under their control;

d. Follow FAA Order 1600.72 when engaging in procurements involving classified information;

e. Appoint in writing:

(1) A Classified Information Security Manger (CISM) for each element that uses, handles, or processes classified information; and

(2) A Classified Information Account Custodians (CIAC) and at least on Alternate Classified Information Account Custodian (ACIAC) to operate the element's Security Control Point and Document Control Stations, if any.

(3) The CISM and CIAC can be the same person.

f. Notify the CISPM when appointing or relieving a CISM CIAC, or ACIAC;

g. Coordinate training for the CISM and others involved in using and handling classified information; and

h. Ensure the performance ratings of these persons include the management of classified information as a critical security element for:

(1) CISMs, and

(2) CIACs and ACIACs

6. Classified Information Security Program Manager (CISPM). The Director, Office of Internal Security and Investigations(AIN-1), is the FAA's CISPM whose responsibilities include:

a. Coordinating training for those who have access to classified information;

b. Providing guidance and support to CISMs through the CISM's Servicing Security Element (SSE). SSEs will answer any questions regarding this order. In the regions your SSE is the Security and Hazardous Materials Division, AXX-700. At the Washington Headquarters, the SSE is the Office of Internal Security and Investigations, AIN-1;

c. Coordinating and overseeing certification and accreditation of National Security Systems owned or used by FAA entities;

d. Coordinating and managing the FAA's classified information inspection program;

e. Coordinating security awareness and education course content;

f. Setting up and coordinating processes to investigate thoroughly information security violations and unauthorized access to classified information;

g. Where possible, recommends measures to correct a classified information violation or compromise;

h. Directing the Personnel Security Program under FAA Order 1600.1 for deciding an FAA employee's eligibility for access to classified information; and

i. Ensuring that FAA employees, who have access to classified information, sign Standard Form 312, Classified Information Nondisclosure Agreement.

7. Classified Information Security Manager. Managers of FAA organizations that create, use, or handle classified information will appoint in writing a CISM. The CISM may be a full-time, part-time, or collateral duty Federal employee. The CISM must hold a security clearance equal to or greater than the highest classification of information held by the organization. The CISM reports directly to the organization's manager on security matters. The CISM also:

a. Carries out this order within their organization;

b. Serves as the principal adviser and representative to management in matters about classifying, declassifying, downgrading, and safeguarding classified information;

c. Limits access to classified information to cleared people with a need-to-know;

d. Keeps a list of personnel within the organization who have access to classified information;

e. Develops and documents the organization's control measures to safeguard classified information and to limit access to classified information to authorized personnel;

f. Develops and keeps certification and accreditation documents for National Security Systems used by their organization;

g. Coordinates with the organization's managers on security measures for classifying and safeguarding classified information;

h. Coordinates information security awareness and education within their organization;

i. In coordination with records management officials, continually reduces classified holdings as appropriate by declassifying, destroying, or retiring unneeded records;

j. Develops written procedures, see Appendix D, specifying how their organization controls and safeguards classified information;

k. Sets up and oversees procedures for any visit involving access to classified information;

l. Reports security violations, including suspected unauthorized access or other threats to safeguarding classified information;

m. Conducts and documents preliminary inquiries of suspected incidents of unauthorized access, loss, or compromise of classified information; and

n. As directed by this order and the CISPM, submits Standard Form 311, Agency Security Classification Management Program Data.

8. National Security Systems (NSS).

a. An *information system* is a discrete set of information resources, either in stand-alone or networked configuration that we organize for the collection, processing, maintenance, transmission, and dissemination of information. National Institute of Standards and Technology Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, states that an information system is an NSS when it has one or more of the following characteristics:

(1) It stores, processes, or communicates classified information;

(2) Its function, operation, or use involves:

(a) Intelligence activities;

(b) Cryptologic activities related to national security;

(c) Command and control of military forces; and

(3) It is an integral part of a weapon or weapons system; or

(4) It is critical to the direct fulfillment of military or intelligence missions and its use is not for routine administrative or business applications.

b. Because NSS are information systems, they must be certified and accredited before we use them to collect, generate, process, store, display, transmit, or receive information. We distinguish NSS because they require different certification and accreditation (C & A) processes from those for other types of information systems. Figure 2-1 shows the C & A process you must use for your NSS.

Figure 2-1, NSS Certification and Accreditation Processes

If you	**Then C & A is by**
Use Sensitive Compartmented Information (SCI) NSS	Director of Central Intelligence (DCI) directives and directives of the agency that sponsors your access to the NSS.
Use terminals that access NSS belonging to a non-FAA entity.	The agency sponsoring and allowing your access to the system, for example, the DoD agency sponsoring you access to the Defense Messaging System (DMS) or the Secret Internet Protocol Router Network (SIPRNET)
Use NSS belonging to the FAA	The C & A process set up by the FAA's ISS Certification Agent

c. Shared responsibility for NSS.

(1) As the SAO, ASH-1 oversees the FAA's program for classifying, declassifying, disclosing, handling, destroying, sharing, and safeguarding classified information. The SAO also coordinates policies and procedures for safeguarding classified information with other lines of businesses, offices, and external agencies.

(2) By FAA Order 1370.82, the Assistant Administrator for Information Services and Chief Information Officer, AIO-1, has overall responsibility for the FAA's Information Systems Security (ISS) Program. AIO-1 also serves as the ISS Certification Agent for all FAA information systems.

(3) By FAA Order 1370.82, heads of lines of business and staff offices must ensure that all information systems within their organizations are certified and accredited. For all FAA-owned or –sponsored NSS, ASH-1 is the Authorizing Official who accredits the NSS.

Chapter 3: CLASSIFICATION MANAGEMENT

1. Classification Standards:

a. The FAA originally classifies information only under these conditions:

(1) An original classification authority (OCA) classifies the information;

(2) The United States Government owns, produces, or controls the information;

(3) The information falls within one or more of these categories:

- Military plans, weapons systems, or operations;
- Foreign government information;
- Foreign relations or foreign activities (including special activities), intelligence sources or methods, or cryptology;
- Foreign relations or foreign activities of the United States, including confidential sources;
- Scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism;
- United States Government programs for safeguarding nuclear materials or facilities;
- Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism; or
- Weapons of mass destructions.

(4) The OCA decides when unauthorized disclosure of the information could result in damage to the national security, and can identify or describe the damage. There is no requirement for the OCA to prepare a written description of such damage. However, OCA's must be able to identify or describe damage in writing, if someone challenges a classification decision or requests classified information under the FOIA.

b. Classification Levels:

(1) *Top Secret* is the term for information, the unauthorized disclosure of which reasonably could be expected to cause *exceptionally grave* damage to the national security. The OCA must be able to identify or describe the exceptionally grave damage.

(2) *Secret* is the term for information, the unauthorized disclosure of which reasonably could be expected to cause *serious damage* to the national security. The OCA must be able to identify or describe the serious damage.

(3) *Confidential* is the term for information, the unauthorized disclosure of which reasonably could be expected to cause *damage* to the national security. The OCA must be able to identify or describe the damage.

(4) We may use *no other terms* to identify United States classified information.

c. You may not automatically declassify classified information because of any unauthorized disclosure of identical or similar information.

d. When there is an unauthorized disclosure of foreign government information, we must presume damage to the national security.

2. FAA Original Classification Authorities.

a. By EO 12958, the Secretary of Transportation may originally classify information as Secret or Confidential and further delegate this authority.

b. Title 49 CFR Part 8.11 further delegates the Secretary's original classification authority to the FAA Administrator. The Secretary must approve delegation of the Administrator's authority to other FAA officials.

3. Requesting Original Classification Authority. FAA officials, who need original classification authority, must ask for the authority *in writing* through the SAO and the Administrator to the Secretary of Transportation. The request must address these issues:

- Why the official needs original classification authority during the normal course of business;
- If enough expertise and information is available to the prospective OCA to allow effective classification decision making;
- Why a classification guide issued by the Administrator would not satisfy the need for original classification authority; and
- Why referral of decisions to existing OCAs is not practical.

4. Specialized Training for Original Classification Authorities. Chapter 6 addresses OCA training.

5. Classification Prohibitions and Limits.

a. Basic Prohibitions and Limits. In no case are we permitted to classify information to:

(1) Conceal violations of law, inefficiency, or administrative error;

(2) Prevent embarrassment to a person, organization, or agency;

(3) Restrain competition; or

(4) Prevent or delay the release of information that does not require protection in the interest of national security.

b. Scientific Research Information and National Security. You may not classify basic scientific research information not clearly related to the national security.

c. Classifying Previously Declassified Information. You may reclassify information after declassification and release to the public under proper authority only under these conditions:

(1) The reclassification action is under the personal authority of the Secretary of Transportation, who decides in writing that reclassification is necessary for national security;

(2) We may reasonably recover the information; and

(3) We report the reclassification action quickly to the Information Security Oversight Office through the DOT Office of Security, M-40.

d. Freedom of Information Act and Privacy Act Requests. The FAA can classify or reclassify FAA information that an authority has not publicly disclosed when we

(1) Receive a request for it under the Freedom of Information Act, the Privacy Act, or the mandatory review rules of EO 12958; and only if

(2) Classification of each requested document meets the requirements of EO 12958, and

(3) The Administrator personally takes part in the classification process.

e. Classification by Compilation. We can classify a compilation of unclassified items of information when the compilation reveals other associations or relationships that:

(1) Meets the standards for classification under EO 12958; and

(2) The individual items of information do not reveal classified information.

6. Derivative Classification. Derivative classification is the act of using classified source information and incorporating, paraphrasing, restating, or creating it in a new form. Source information normally consists of a classified document or documents, or a classification guide issued by an OCA.

a. Derivative Classification Authority. People who reproduce, extract, or summarize classified information, or who apply classification markings drawn from source material or a classification guide are derivative classifiers. They get authority to classify information from classification guides or other classified documents.

b. Developing Derivative Material**.** Classification guides and other classified source documents specify items of classified information and the duration of classification for each item.

c. FAA Derivative Classifiers. Within the FAA people who incorporate, paraphrase, restate, or create in new form - *already classified information* - have *derivative* classification authority. The Administrator is the only FAA official, who has *original* classification authority.

d. Derivative Classification Duties. Derivative classifiers must:

(1) Follow and respect original classification decisions; and

(2) Carry forward to any newly created documents the relevant classification markings. For information derivatively classified based on multiple sources, the derivative classifier will carry forward:

- The date or event for declassification that matches to the longest period of classification among the sources; and
- A listing of these sources on each copy of their new document.

7. Exceptional Classification Decisions. When an FAA employee, who does not have original classification authority, originates information the employee considers classified, the employee will:

a. Treat Information Like a Classified Working Paper. Mark and safeguard the information in the manner prescribed for a working paper; and

b. Properly Send the Working Paper to the SAO. The SAO will coordinate with the proper subject matter and classification authority for an original classification decision.

8. Duration of Classification.

a. Specific Date or Event. When classifying information, an OCA fixes a specific date or event for declassification based on the duration of the national security sensitivity of the information. The date or event must not exceed the time frames of paragraph 8.b., below.

b. 10-Year Rule. If an OCA cannot fix an earlier declassification date or event, the declassification date is 10 years from the day of the original decision. That is unless the OCA decides the information's sensitivity needs a later declassification date - up to 25 years from the date of the original decision. The automatic declassification rules of EO 12958 apply to all 25-year old records of permanent historical value under Title 44, United States Code.

c. Extending Duration. An OCA may extend classification duration, change classification levels, or reclassify specific information only under the standards and procedures for classifying information of EO 12958.

d. Extensions of classification are not automatic. When information has a declassification date or event, you declassify it on the date or event unless the responsible OCA extends the date or event. Responsible OCAs may extend declassification durations for periods not exceeding 10 years at a time if the declassification date or event is 10 years or less from the classification date.

e. Records of Permanent Historical Value. For information in records having permanent historical value, successive extensions may not exceed 25 years from the date of the information's origin. Section 3.3 of EO 12958 governs continued classification of information beyond 25 years.

f. Records Not Having Permanent Historical Value. For information in records not determined to have permanent historical value, successive extensions may exceed 25 years from the date of the information's origin.

g. Conditions for extending classification. When extending the duration of classification, the original classification authority must:

(1) Be the original classification authority with jurisdiction over the information;

(2) Ensure the information continues to meet the standards for classification under EO 12958; and

(3) Make reasonable tries to notify all known holders of the information.

h. Information classified under prior executive orders:

(1) Specific date or event. Unless declassified earlier, you declassify information marked with a specific date or event for declassification under a prior EO on the specific date or event. This rule does not apply to permanently valuable records as determined by the Archivist of the United States. Section 3.3 of EO 12958 applies to declassifying these records when their declassification date or event is more than 25 years from the information’s origin.

(2) Indefinite duration of classification. For information marked "Originating Agency's Determination Required, its acronym “OADR,” or with some other marking of an indefinite duration of classification under a prior order:

(a) A declassification authority, as defined EO 12958, may declassify it;

(b) An OCA with jurisdiction over the information may remark the information to fix a duration of classification consistent with the requirements for information originally classified; or

(c) Unless declassified earlier, *permanently valuable* records remain classified for 25 years from the date of their origin. Then they are subject to Section 3.3 of EO 12958.

(3) Foreign government information (FGI). The declassifying agency is the agency that initially received or classified the information. When declassifying FGI that you hold, you must find out if a treaty or agreement applies to it that would prevent its declassification. Depending its age and whether it’s a *permanently valuable* record, you

must also decide if another exemption under EO 12958 applies to the information. If you believe other exemptions apply, you should consult with other concerned agencies in making a declassification determination. You or the Department of State, as fitting, should consult with the foreign government before declassification. See Appendix C for further information.

i. Deciding When Information Is Subject to Declassification. We base our decisions on when we first recorded the information in our record's system. The following examples explain these decisions:

Example 1. The FAA first issues a classification guide on FAA Support to Classified Military Plans and Operations on October 20, 1995. The guide states that we must classify a certain fact at the Secret level for ten years. We classify a document dated July 10, 1999, because it includes this fact from the October 20, 1995 classification guide. We mark the document for declassification on October 20, 2005. This is ten years after the fact appears in the guide, not on July 10, 2009, ten years after we derivatively created the classified document.

Example 2. The same FAA classification guide states that we must classify an event at the Secret level for ten years after the event occurs. The event first occurs on July 10, 1999. We mark the document for declassification on July 10, 2009, ten years after the event occurs, and not on October 20, 2005, ten years after the date of the guide's generic instruction.

9. Classification Challenges. EO 12958 allows holders of classified information to challenge classifications as a means for promoting proper and thoughtful classification actions. Agencies will take no retribution against an authorized holder for challenging classifications in good faith.

a. FAA Procedures:

(1) Holders of FAA classified information, who wish to challenge the classification status of information, will make their challenge in writing to the SAO through their Servicing Security Element (SSE). The written challenge need not be any more specific than to question why we did or did not classify information, or why we classified the information at a certain level.

(2) The SAO will set up procedures for processing, tracking and recording formal classification challenges. Freedom of Information Act (FOIA) requests for classified information are not formal classification challenges, and we handle, track, and record FOIA requests under FAA Order 1270.1.

(3) The SAO will provide the challenger with:

(a) A written response to a challenge within 60 days, or

(b) A written acknowledgment that we received the challenge with a date by which the challenger can expect a response. The acknowledgment will include a statement that if we do not respond within 120 days, the challenger has the right to send the challenge to the Interagency Security Classification Appeals Panel for a decision. The challenger may also forward the challenge to the Interagency Security Classification Appeals Panel if the SAO has not responded to an internal appeal within 90 days of the SAO's receipt of the appeal. SAO responses to denied challenges will include the challenger's appeal rights to the Interagency Security Classification Appeals Panel.

(4) If a classification challenge has been the subject of another challenge within the past two years, or is the subject of pending litigation, we will tell the challenger of this fact and of the challenger's appeal rights, if any.

(5) Challengers and the SAO will try to keep all challenges, appeals and responses unclassified. However, we will handle and protect classified information contained in a challenge, a response, or an appeal under EO 12958 and its implementing directives. Also it remains classified until we make a final decision to declassify it.

b. Informal Challenges and Questions. The FAA encourages informal questioning of the classification status of particular information by authorized holders of information as a means of holding down the number of formal challenges. Send your question to your SSE, who will research and answer your question.

10. FAA Classification Guides. A classification guide consists of predetermined classification decisions by an OCA. Classification guides are primary reference sources for derivative classifiers. As the FAA's OCA, the Administrator issues classification guides to identify the FAA's recurring classification decisions.

a. The SAO coordinates preparation of FAA classification guides. Coordination includes:

(1) Consulting with users of guides when developing or updating guides;

(2) Communicating within the FAA and with other agencies that are developing similar guidelines to ensure the consistency and uniformity of classification decisions;

(3) Getting OCA approval; and

(4) Keeping a list of FAA classification guides.

b. Classification guide content. At a minimum classification guides must:

(1) Identify the subject matter of the classification guide;

(2) Identify the original classification authority by name or personal identifier, and position;

(3) Identify an agency point-of-contact or points-of-contact for questions about the classification guide;

(4) Provide the date of issuance or last review;

(5) Precisely describe the items of information that need protection;

(6) State which classification level applies to each item of information, and, when useful, specify the unclassified items of information;

(7) State, when applicable, special handling warnings;

(8) Prescribe declassification instructions or the exemption category from automatic declassification for each item of information;

(9) When exempting information from automatic declassification, cite the exemption category from section 3.3 of EO 12958, the applicable statute, treaty or international agreement; and

(10) State a concise reason for classification which, at a minimum, cites the applicable classification category or categories.

c. Distribution of classification guides. The FAA shares its classification guides with potential user as necessary to ensure the proper and uniform derivative classification of FAA information.

d. Reviewing and updating classification guides:

(1) The SAO reviews and updates FAA classification guides, including guides created under prior orders, when our classification decisions change or every five years. Updated instructions for guides first created under prior orders will comply with EO 12958.

(2) The SAO will consult the users of guides when reviewing or updating them. Also, users of classification guides should inform the SAO when they learn of information that suggests the need for changing a guide.

e. Marking and safeguarding classification guides:

(1) We do not classify them, unless they contain classified information.

(2) We mark them For Official Use Only or Sensitive Security Information, as appropriate, to control their release outside the FAA and their dissemination within the FAA. (FAA Order 1600.75)

Chapter 4: IDENTIFICATION AND MARKING

1. General Requirements. This chapter gives instructions for identifying and marking classified information.

a. Basic marking requirements. When originally classifying information, the following must appear on the face of each classified document, or in a similar manner on other classified media:

(1) One of the three classification levels: "Top Secret," "Secret," or "Confidential";

(2) The identity, by name or personal identifier and position, of the original classification authority;

(3) The agency and office of origin, if not obvious;

(4) Declassification instructions, which must show one of the following:

- The date or event for declassification;
- The date that is 10 years from the date of original classification; or
- The date that is up to 25 years from the date of original classification; and
- A concise reason for classification that cites, at a minimum, the applicable classification categories of EO 12958.

b. Omitting specific declassification instructions. Classifiers may omit specific declassification instructions if the instruction would reveal classified information.

c. Portion marking. Classifiers must point out by marking or other means, which portions they classify, with the applicable classification level, and the portions they do not classify. Only the Director of the Information Security Oversight Office may grant waivers of portion marking.

d. Foreign government information. Foreign government information must keep its original classification markings or must have a U.S. classification that provides a degree of protection at least equivalent to that required by the government that provided the information. We do not need to assign U.S. classification markings to foreign government information when the foreign government markings are enough to meet the purposes served by U.S. classification markings.

e. Omission of required markings. When EO 12958 or a predecessor order assigns a classification level to information, we consider that information classified at that level despite omissions of other required markings. Whenever we use such information in derivative classification or we review it for possible declassification, we must coordinate with the original classification authority for omitted markings.

f. Classified addenda. Classifiers should use a classified addendum whenever classified information forms a small portion of an otherwise unclassified document.

g. Public release of declassified records. Before public release, classifiers must correctly mark all declassified records to reflect their declassification.

2. FAA Marking Policy. Classifiers must mark classified information with standard markings. Except in extraordinary circumstances, classified information created after March 25, 2003 (the effective date of EO 13292), will not deviate from the following marking formats. If classifiers cannot mark specific classified information or materials, the classifier must provide holders or recipients of the information with written instructions for protecting the information. Classifiers will uniformly and visibly mark information to leave no doubt about the classified status of the information, the protection level needed, and the duration of classification.

3. Original Classification Markings. On the face of each originally classified document, including electronic media, the classifier must apply the following markings:

a. Classification authority. The name or personal identifier, and position title of the original classifier must appear on the "Classified By" line. An example might appear as:

Classified By: Marion C. Blakey, Administrator, AOA-1

b. Agency and office of origin. If not obvious, original classifiers must identify and place the agency and office of origin below the name on the "Classified By" line. An example might appear as:

Classified By: Marion C. Blakey, Administrator, AOA-1
FAA, Office of the Administrator

c. Reason for classification. The original classifier must identify the reasons for the decision to classify. The classifier must include, at a minimum, a brief reference to the relevant classification categories, or the number 1.4 plus the letters that matches the classification category in section 1.4 of EO 12958.

(1) These categories, as they appear in EO 12958, are:

1.4a - military plans, weapons, or operations;

1.4b - foreign government information;

1.4c - intelligence activities (including special activities), intelligence sources or methods, or cryptology;

1.4d - foreign relations or foreign activities of the United States, including confidential sources;

1.4e - scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism;

1.4f - United States Government programs for safeguarding nuclear materials or facilities; or

1.4g - vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans or protection services relating to the national security, which includes defense against transnational terrorism; or

1.4h – weapons of mass destruction.

(2) An example might appear as:

Classified By: Marion C. Blakey, Administrator, AOA-1
FAA, Office of the Administrator
Reason: 1.4g, Vulnerabilities or capabilities of systems, installations

(3) When classification reasons are not clear from the content of the information, for example, classification by compilation, the classifier must provide a more detailed explanation of classification reasons.

d. Declassification instructions**.** Classifier must place the duration of the original classification decision on the "Declassify On" line as shown below:

(1) The classifier will apply a date or event for declassification that matches the duration of the information's national security sensitivity, which may not exceed 10 years from the date of the original decision. When linking the duration of classification to a specific date or event, state the date or event as:

Classified By: Marion C. Blakey, Administrator, AOA-1
FAA, Office of the Administrator
Reason: 1.4g, Vulnerabilities or capabilities of systems, installations
Declassify On: October 14, 2009 or
Declassify On: Completion of Operation

(2) When unable to fix a specific date or event within 10 years, the classifier will apply the date that is 10 years from the date of the original decision. For example, on a document that contains information classified on October 14, 2004, mark the "Declassify On" line as:

Classified By: Marion C. Blakey, Administrator, AOA-1
FAA, Office of the Administrator
Reason: 1.4g, Vulnerabilities or capabilities of systems, installations
Declassify On: October 14, 2014

(3) If the OCA cannot fix an earlier specific date or event for declassification, the OCA will mark it for declassification 10 years from the date of the original decision. The OCA may waive the “10-year rule” when the sensitivity of the information needs longer

classification for up to 25 years from the date of the original decision. All information marked for declassification 25 years from the date of the original decision is subject to section 3.3 of EO 12958 if the information is in records of permanent historical value under title 44, United States Code.

(4) An original classification authority may extend the duration of classification, change the classification level, or reclassify specific information only when following the standards and procedures for classifying information under EO 12958.

4. Overall Markings. The highest classification level for information contained in a document must appear in a way that will distinguish it clearly from the informational text.

a. Document covers, title page, and first page. Prominently place the overall classification at the top and bottom of the face of the front cover (if any), on the title page (if any), on the first page, and on the rear of the back cover (if any).

b. Different levels of classification. For documents containing information classified at more than one level, mark the document at its highest classification level. For example, if a document contains some information marked “Secret” and other information marked “Confidential,” the overall marking is “Secret.”

c. Interior pages. Mark each interior page of a classified document at the top and bottom, either

(1) With the highest classification level for information contained on that page, including the marking “Unclassified” when it is applicable, or

(2) With the highest overall classification of the document.

5. Portion Markings. Classifiers must mark each portion of a document, usually a paragraph, but including subjects, titles, graphics and the like, to point out its classification level by placing a parenthetical symbol immediately preceding or following the portion to which it applies.

a. Portion symbols. Use the symbols “(TS)” for Top Secret, “(S)” for Secret, “(C)” for Confidential, and “(U)” for Unclassified.

b. Requests to waive portion marking. The Senior Agency Official (SAO) only may waive portion marking for a specific category of information. Classifiers may request a waiver – in writing – through their chain of command - to ASH-1.

6. Classification Extensions. Classification extension markings:

a. Ten year extension. An original classification authority may extend the duration of classification for successive periods not to exceed 10 years at a time. For information contained in records determined to be permanently valuable, multiple extensions must not exceed 25 years from the date of the information's origin.

b. Identity of the person authorizing extension. When extending declassification you must revise the "Declassify On" line to include the new declassification instructions, the identity of the person approving the extension, and the date of the action.

c. Extension notification. The SAO will notify all known holders of the information and will update classification guides to reflect such revisions. An example:

Classified By: Marion C. Blakey, Administrator, AOA-1
FAA, Office of the Administrator
Reason: 1.4g, Vulnerabilities or capabilities of systems, installations
Declassify On: Classification extended on December 1, 2000, until
December 1, 2010, by Marion C. Blakey, Administrator, FAA

7. Derivative Classification Marking. Information classified derivatively based on source documents or classification guides must bear all markings prescribed above, except as provided in this paragraph. Derivative classifiers must carry forward markings from the source document or take it from instructions in a classification guide.

a. Source of derivative classification.

(1) The derivative classifier must concisely identify the source document or the classification guide on the "Derived From" line, including the agency and, where available, the office of origin, and the date of the source or guide. For example:

Derived From: Memo, "Funding Problems, '' Oct. 20, 1995, Ofc. of Admin., Department of Transportation or

Derived From: Classification Guide No. 1, Department of Transportation, of Oct. 20, 1995

(2) When a classifier uses more than one source document or classification guide to classify a document, the "Derived From" line must appear as:

Derived From: Multiple Sources

(3) The derivative classifier must identify each source document on each copy of a derivatively classified document.

(4) A document derivatively classified based on a “Multiple Sources” document must cite the source document on its "Derived From" line rather than the term "Multiple Sources." For example:

Derived From: Report entitled, "Security Shortfalls", dated Oct. 20, 1995, Department of Transportation, Office of Administration

b. Reason for classification. When derivatively classifying a document, derivative classifiers do not need to transfer the reason for the original classification decision, as shown in the source documents or classification guide. However, if the classifier includes the reason for original classification, the marking must conform to the standards for original classification.

8. Derivative Declassification Instructions.

a. Carry forward instructions of source document. Derivative classifiers must carry forward the instructions on the "Declassify On" line from the source document to the derivative document, or the duration instruction from the classification guide.

b. Carrying forward instructions of multiple source documents. When derivatively classifying a document based on more than one source document or more than one element of a classification guide, the "Declassify On" line must reflect the longest duration of any of its sources.

c. Carrying forward instructions for originating agency's determination required. When derivatively classifying a document from source documents or classification guide that contains the declassification instruction, "Originating Agency's Determination Required, '' or "OADR, '' unless otherwise directed by the original classifier, the derivative classifier must carry forward:

(1) The fact the source documents carried the OADR instruction; and

(2) The date of origin of the most recent source documents, classification guide, or specific information, as suitable to the circumstances. For example:

Declassify On: Source marked "OADR", Date of source: October 20, 1990

This marking suggests when the classified information is 25 years old and, if permanently valuable, subject to automatic declassification under section 3.4 of EO 12958.

d. Overall marking. The derivative classifier must clearly mark the classified document with the highest classification of information included in the document.

e. Portion markings. The derivative classifier must mark each portion of a derivatively classified document as marked in the source material.

9. Other Marking Requirements.

a. Marking prohibitions. Classifiers must not use the following:

(1) Markings other than "Top Secret," "Secret," and "Confidential" to identify classified national security information;

(2) Other terms, special markings, or phrases such as “Secret Sensitive” or “Agency Confidential” to identify classified national security information; or

(3) The terms “Top Secret,” “Secret,” and “Confidential” to identify nonclassified executive branch information.

b. Transmittal documents. A transmittal document must show on its face the highest classification of any classified information attached or enclosed. The transmittal must also include prominently on its face the following or similar instructions:

Unclassified When Classified Enclosure Removed or On Removal of Attachments, This Document is (Classification Level)

c. Foreign government information.

(1) Documents that contain foreign government information will include the marking: “This Document Contains (show country of origin) Information.”

(2) Classifiers must mark the portions of the document that contain the foreign government information to point out the government and classification level. For example if the portion contains United Kingdom Confidential, then mark the portion “(UK-C).”

(3) If a classifier must conceal the identity of the specific government, then:

(a) Include the marking, “This Document Contains Foreign Government Information;”

(b) Mark relevant portions with “FGI” and the classification level, for example, “(FGI-C).” and

(c) Keep a separate record that identifies the foreign government to help later declassification actions.

(4) When the FAA transfers classified records to the National Archives and Records Administration for storage or archival purposes, the accompanying documentation must, at a minimum, identify the boxes that contain foreign government information. If we must conceal the fact that information is foreign government information, then we must not use the markings described in this paragraph, but we must mark the document as if it were of U.S. origin.

10. Compilations. Compilations are combinations of unclassified information that reveal classified information. When marking compilations:

a. Introductory statement. Begin the document with a statement on how the compilation results in classified information.

b. Overall marking. Mark the top and bottom of each page and the outside of any front or back cover.

c. Portion marking. Mark unclassified portions with a "(U)" at the beginning of each unclassified portion.

d. Unclassified attachments. Do not mark unclassified attachments with any markings that might reveal its relationship to an unclassified compilation.

11. Working Papers. Working papers are documents or materials, regardless of the media, which we expect to revise into a finished product for distribution or retention.

a. When creating working papers. Classifiers must follow procedures set up by their Classified Information Security Manager for creating and marking working papers to include:

- Dating them;
- Marking them with the highest classification of any information they contain;
- Protecting them at that level; and
- Destroying them when no longer needed.

b. When to control working papers as finished documents. When any of these conditions apply, we must control and mark working papers the same as finished documents:

- Released outside the originator's organization;
- Held more than 180 days from the date of origin; or
- Filed permanently.

12. Marking Other Material.

a. Bulky material. Classifiers must clearly identify bulky material, equipment, facilities, and items in a manner that leaves no doubt about their classified status, the protection level needed, and the duration of classification. If you find that identification would itself reveal classified information, then do not include such identification. You must keep supporting documentation for our finding in the appropriate security facility and in any applicable classification guide.

b. Classified communications security (COMSEC) material. Follow FAA Order 1600.8.

13. Unmarked Materials. If we hold unmarked records about the national defense or foreign relations of the United States and are protecting them as classified information under prior EOs, we must:

a. Continue to treat them as classified information under EO 12958, and

b. Subject them to declassification rules of EO 12958.

14. Marking Guide. For specific examples of how to mark classified materials:

- Go to Your Work Tools on the FAA Employee Intranet;
- From Your Work Tools Menu go to the Security and Hazardous Materials menu; and
- Click on Marking Classified National Security Information.

Chapter 5: INSPECTIONS

1. Inspection Overview. By E.O. 12858, the FAA must set up and manage an inspection program to measure our performance for classifying, declassifying, and safeguarding classified information. This chapter assigns responsibilities and sets standards for our inspection program which includes review and assessment of our classified products.

2. Responsibilities:

a. Senior Agency Official (SAO), ASH-1. The SAO oversees the inspection program.

b. Director, Office of Internal Security and Investigations, AIN-1. AIN-1 develops inspection guidelines and procedures.

c. Servicing Security Elements (SSE). SSEs will conduct yearly inspections of security control points, report inspection results, and oversee corrective actions.

3. Conduct of Inspections. Inspections will include, but are not limited to reviews of:

a. Safeguarding procedures. Classified information marking, handling, processing, storage, transmission, distribution, and destruction.

b. Access and accountability controls. Access and control procedures and records.

c. Security awareness and education. Evaluating the effectiveness of our security awareness, and education program for those who handle classified information.

4. Inspection Standards. Title 32 CFR Part 2001.61 and Chapter 6 form our basic inspection standards.

Chapter 6: SECURITY AWARENESS AND EDUCATION

1. General. This chapter sets goals and standards for classified information security awareness and education.

2. Security Awareness and Education Goals:

a. FAA employees. Ensure that all FAA employees who create, process, or handle classified information have a satisfactory knowledge and understanding about classification, safeguarding, and declassification policies and procedures;

b. Consistency. Set up uniform awareness, education, and training products; and

c. Promote sound classified information security practices. Promote proper classification, safeguarding, and declassification practices and reduce errors.

3. Standards:

a. EO 12829, the National Industrial Security Program (NISP). The National Industrial Security Program Operating Manual (NISPOM), Department of Defense Manual a 5220.22-M set up the NISP and prescribes the security requirements, limits, and safeguards applicable to industry, including the conduct of contractor security education and training.

b. EO 12958 and Subpart F of Title 32 CFR 2001. These set the basic standards for security awareness and education.

c. Senior Agency Official (SAO), ASH-1. The SAO delegates to the ASH-20 Manager responsibility to decide the means and methods for providing security awareness and education. Delivery methods may include live briefings, interactive video teletraining (IVT); computer based training, videos, and so on.

d. Records.

(1) Servicing Security Elements keep records, Standard Form 312, on Initial and Termination briefing, and

(2) Classified Information Security Managers keep attendance records for cleared personnel who attend annual refresher briefings.

4. Security Awareness and Education Products:

a. Initial briefing. All cleared employees will receive an initial briefing on basic security policies, principles and practices, and criminal, civil, and administrative penalties. This briefing normally happens with granting a security clearance, and before granting access to classified information. The person receiving the briefing will sign a Classified Information Nondisclosure

Agreement, Standard Form (SF) 312, if their SF 312 is not on file with the FAA. The initial briefing includes:

(1) Roles and responsibilities:

- What are the responsibilities of the Senior Agency Official and other FAA management officials?
- What are the responsibilities of FAA employees who create or handle classified information?
- Who to contact with questions or concerns about classification matters?

(2) Elements of classifying and declassifying information.

(3) What classified information is and why it's important to protect it?

(4) What are the levels of classified information and the damage criteria associated with each level?

(5) What are the prescribed classification markings and why is it important to have classified information fully and properly marked?

(6) What are the general requirements for declassifying information?

(7) What are the procedures for challenging the classification status of information?

(8) Elements of safeguarding:

- What are the proper procedures for safeguarding classified information?
- What is an unauthorized disclosure and what are the criminal, civil, and administrative penalties associated with these disclosures?
- What are the general conditions and controls for access to classified information?
- What should an individual do when they know of a security violation?

b. Specialized security awareness and education. Original classifiers, declassification authorities, individuals specifically appointed as responsible for derivative classification, classification management officers, security managers, security specialists, and all other personnel whose duties significantly involve the creation or handling of classified information will receive more detailed training. This training should occur before or concurrent with the date the employee assumes any of the positions listed above, but in any event by six months from then. Training will include:

(1) Classification and Marking.

- What is the difference between original and derivative classification?
- Who can classify information originally?
- What are the standards that a classifier must meet to classify information?

- What discretion does the OCA have in classifying information, for example, foreign government information?
- What is the process for fixing duration of classification?
- What are the prohibitions and limits on classifying information?
- What are the basic markings that must appear on classified information?
- What are the general standards and procedures for declassification?

(2) Declassification.

- What are the standards, methods and procedures for declassifying information under EO 12958, as amended?
- What are the standards for creating and using agency declassification plans?
- What an agency's automatic declassification plan covers?
- What are the FAA's responsibilities for keeping a declassification database?

(3) Individuals specifically appointed as security managers, classification management officers, security specialists, or anyone whose duties significantly involve the creation or handling of classified information.

- What are the original and derivative classification processes and the standards applicable to each?
- What are the proper and complete classification markings, as described in EO 12958 and 32 CFR Part 2001?
- What are the authorities, methods, and processes for downgrading and declassifying information?
- What are the methods for the proper use, storage, reproduction, transmission, disclosure, and destruction of classified information?
- What are the requirements for creating and updating classification and declassification guides?
- What are the requirements for controlling access to classified information?
- What are the procedures for investigating and reporting security violations, and the penalties associated with such violations?
- What are the requirements for creating, maintaining, and terminating special access programs, and the mechanisms for overseeing such programs?
- What are the procedures for the secure use, certification and accreditation of automated information systems and networks which use, process, store, reproduce, or transmit classified information?
- What are the requirements for oversight of the security classification program, including agency self-inspections?

c. Refresher security awareness and education. Employees who create, process or handle classified information will receive a refresher briefing training yearly, and CISMs will keep attendance records of employees who receive this training. Refresher briefings will:

- Reinforce the policies, principles and procedures covered in initial and specialized training;
- Address the threat and the techniques employed by foreign intelligence activities to get classified information;
- Advise personnel of penalties for engaging in espionage; and
- Also address issues or concerns identified during inspections.

d. Termination briefings. Each employee granted access to classified information who leaves the FAA or who has their clearance withdrawn will receive a termination briefing. When possible the briefer will use the employee's Standard Form 312 for briefing content and documentation. At a minimum, termination briefings must impress on each employee:

- Their continuing responsibility not to disclose any classified information to which the employee had access and the potential penalties for noncompliance; and
- Their duty to return to their Classified Information Account Custodian all classified documents and materials in their possession.

e. Other security awareness and education:

- Practices applicable to FAA officials traveling overseas;
- Procedures for protecting classified information processed and stored in automated information systems;
- Methods for dealing with uncleared personnel who work near classified information;
- Responsibilities of personnel serving as couriers of classified information; and
- Security requirements that govern participation in international programs.

Chapter 7: DECLASSIFICATION OF CLASSIFIED INFORMATION

1. Declassification Overview. Declassification decisions fix the duration of protection and are as important as the decisions to classify information. This chapter addresses:

a. National and DOT regulations about declassification;

b. Declassification policies and principles;

c. FAA declassification authorities; and

d. FAA declassification processes.

2. National and DOT Declassification Regulations and Orders:

a. Title 32 CFR 2001 Subpart C. Information Security Oversight Office (ISOO), Classified National Security Information Directive No. 1; and

b. Title 49 CFR Part 8. Classified Information: Classification/Declassification/Access.

3. Declassification Policies and Principles:

a. No longer meets classification standards. Under Section 3.1 of EO 12958, you must declassify information when it no longer meets EO 12958 standards for classification.

b. Derivative declassification instructions. Derivative classifiers will carry forward declassification and downgrading instructions from source documents.

c. Follow declassification instructions. When information carries markings for downgrading or declassification, you do not need further authority to downgrade or declassify it.

d. Unauthorized disclosure. The FAA does not automatically declassify information because of unauthorized disclosure of identical or similar information.

e. Overriding public interest. In exceptional cases the public interest in certain classified information may outweigh the need to protect it. When these cases arise, refer them to the SAO, who in collaboration with OCAs will:

(1) Decide whether the public interest reasonably outweighs the damage to the national security from its disclosure, if the FAA originally classified the information; or

(2) If another agency originally classified the information, coordinate the case with that agency.

f. Declassification by Redaction. Redacting is the editing, taking out, or sanitizing of classified information from a document to declassify the document so we can release it without

disclosing classified information. You may redact classified information from a classified document and declassify it when:

(1) The classified information comprises a small portion of the document, and

(2) Redaction does not clearly distort the overall meaning or informational value of the document.

g. Redaction standards:

(1) Hard copies. Regardless of the method you use, the method must be effective to ensure that the redacted classified information cannot still be read. “Blacking out” methods using magic markers or grease pencils are ineffective because they leave latent images. An effective method is covering the classified information completely with opaque labels, tape, or Post-it notes, and then making a copy the document.

(2) Soft copies. The Information Security Directorate of the National Security Agency has issued guidance for reacting Word and Adobe documents. You can find this guidance on the Internet by searching for Report #I333-015R-2005, Redacting with Confidence: How to Safely Publish Sanitized Reports Converted From Word to PFD.

(3) If you need help with redacting a document, contact your Servicing Security Element (SSE).

h. Transfer of function. When the FAA receives classified information in a transfer of function and not merely for storage, the FAA becomes the originating agency. We may declassify or downgrade the information after consultation with other agencies having an interest in the subject matter.

i. Records of permanent historical value. FAA reviews records having permanent historical value for declassification before sending them to the National Archives and Records Administration (NARA).

j. Foreign government information. When foreign government information is subject to declassification, the SAO finds out if the information is also subject to a treaty or international agreement that would prevent its declassification. The SAO also finds out if another exemption applies under EO 12958, such as the United States foreign relations exemption. If such an exemption applies, the SAO will consult with any other concerned agencies in making its declassification determination. The FAA will coordinate with the Department of State about who should consult with the foreign government before declassification.

k. Role of Information Security Oversight Office. If the Director of the ISOO decides that the FAA violated EO 12958 while classifying information, the Director may demand that we declassify the information. We may appeal the Director’s decision, and the information remains classified awaiting a decision on our appeal.

4. Declassification Authorities. Officials who have original classification authority also have declassification authority. In addition the Transportation Secretary delegates declassification authority to other officials who manage agency declassification processes. The Secretary has delegated this authority to these FAA officials:

a. Assistant Administrator for Security and Hazardous Materials, ASH-1 and

b. Deputy Assistant Administrator for Security and Hazardous Materials, ASH-2

5. Declassification Processes. EO 12958, as amended sets up declassification processes, and the SAO is responsible for coordinating and managing them.

a. Original declassification instructions. These instructions declassify information based solely on:

(1) A specific date or event as determined by an OCA; and

(2) A specific time frame for duration of classification as set up by EO 12958.

b. Automatic declassification. EO 12958 states that NARA must automatically declassify a classified record, unless the Secretary of Transportation exempts the record from automatic declassification, when:

(1) The record is more than 25 years old; and

(2) Is of permanent historical value under Title 44, United States Code.

c. Systematic declassification. Systematic Declassification involves reviewing our classified records that are exempt from automatic declassification and are in the care of NARA.

d. Automatic and systematic declassification plan**.** The SAO in coordination with the Director, DOT Office of Security, M-40, and NARA will develop a plan for regular reviews of FAA documents held in NARA archives.

e. Mandatory declassification. This process involves reviewing classified information in response to a request for declassification.

6. Original Declassification Instructions.

a. Original declassification decision. When originally classifying information, an OCA decides the duration for which classification will continue. This decision is an essential part of the original classification, and the OCA bases the decision on the national security sensitivity of the information. We declassify the information, on reaching the date or event.

b. "10 - Year Rule". If the OCA cannot fix an earlier specific date or event for declassification, the OCA must mark the information for declassification 10 years from the date of the original classification decision.

c. "10 – Year Rule" exceptions. The OCA may reasonably decide the information needs longer protection. If this is the case, you may mark the information for declassification for up to 25 years from the date of original classification. Reasonable exception conclusions include:

(1) The OCA expects that unauthorized disclosure of the information could cause damage to the national security for a period more than 10 years; and

(2) The release of the information could:

- Reveal the identity of a confidential human source, or a human intelligence source, or reveal information about applying intelligence source or method;
- Reveal information that would assist in the development of use of weapons of mass destruction;
- Reveal information that would impair U.S. cryptologic systems or activities;
- Reveal information that would impair the application of state of the art technology within a U.S. weapon system;
- Reveal actual U.S. military war plans that remain in effect;
- Reveal information, including foreign government information, that would seriously and demonstrably impair relations between the U.S. and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the U.S.;
- Reveal information that would clearly and demonstrably impair the current ability of the U.S. Government officials to protect the President, Vice President, and other protectees for whom protection services, in the interests of national security, are authorized;
- Reveal information that would seriously and demonstrably impair current national security preparedness plans or reveal current vulnerabilities of systems, installations, infrastructures, or projects relating to the national security; or
- Violate a statute, treaty, or international agreement.

7. Automatic Declassification.

a. December 31, 2006. On this date EO 12958 automatically declassifies all classified records held by NARA that are more than 25 years old and are of permanent historical value under Title 44 U.S.C. Subsequently, EO 12958 automatically declassifies all classified records on December 31 of the year that is 25 years from the date of its original classification unless the Secretary of Transportation exempts the records by Section 3.3 of EO 12958.

b. Exemption requests. The FAA must ask the Secretary of Transportation to exempt a record from automatic declassification no later than 195 days before the record's 25th anniversary.

c. Information exempt from automatic declassification. Classified information exempt from automatic declassification are subject to mandatory and systematic declassification processes.

d. Records not held by NARA**.** Classified records, not scheduled for disposal or retention by NARA, are not subject to this process.

e. Restricted Data and Formerly Restricted Data.

(1) EO 12958 exempts Restricted Data (RD) and Formerly Restricted Data (FRD) records from automatic declassification because the Atomic Energy Act of 1954, as amended, classifies these records. Restricted Data concerns:

- The design, manufacture, or utilization of atomic weapons;
- The production of special nuclear material, for example, enriched uranium or plutonium; or
- The use of special nuclear material in the production of energy.

(2) Formerly Restricted Data is information that is still classified but which has been removed from the Restricted Data category because it relates primarily to the military use of atomic weapons.

(3) Any document marked Restricted Data or Formerly Restricted Data must remain classified indefinitely, or we must refer it to the Department of Energy or the Department of Defense for a classification review.

8. Systematic Declassification.

a. FAA classified records. If the FAA is the originating agency for records of permanent historical value, which the Secretary of Transportation has exempted from automatic declassification, the SAO will set up a systematic declassification program for those records.

b. Declassification guides. The program will include declassification guidelines that:

(1) Identifies the subject matter of the declassification guide;

(2) Identifies the original classification authority;

(3) Provides the date of issuance or last review;

(4) States the categories or items we must declassify or downgrade; and

(5) Identifies any file series exempt for automatic disclosure.

c. Coordinating declassification guides. The SAO forwards our declassification guides to ISOO through the DOT Director of Security, M-40.

9. Mandatory Declassification. Information classified by the FAA is subject to a mandatory declassification review in a response to a request for the information. The SAO will coordinate the review by the procedures of Title 49 CFR Parts 8.15 through 8.21.

Chapter 8: UNAUTHORIZED ACCESS, LOSS, OR COMPROMISE OF CLASSIFIED INFORMATION

1. Unauthorized Access, Loss, or Compromise Policy.

a. Take immediate action. Unauthorized access, loss, or compromises of classified information pose serious threats to national security. When we suspect unauthorized access, loss, or compromise of classified information we must take immediate action to address potential threats. Immediate action means quickly reporting and looking into suspected incidents to:

(1) Negate or mitigate adverse effects of the incident;

(2) Find out if we compromised classified information and, if so, if there is damage to national security; and

(3) Find out the people and conditions that contributed to the incident.

b. Reporting duty. FAA employees or contractors who know of a possible loss, compromise, or unauthorized disclosure of classified information must immediately report the incident to their supervisor and Classified Information Security Manager (CISM).

c. Cryptographic information. We handle incidents involving cryptographic information by FAA Order 1600.8.

d. Employee duties. Employees finding unprotected classified material will:

(1) Take custody of and safeguard it if possible; and

(2) Immediately report the incident to his or her supervisor and the CISM.

e. Media relations. If classified information appears in the public media, employees will not make any statement or comment that would confirm the accuracy or corroborate the classified status of the information. Employees will refer any media questions or inquiries to the appropriate FAA public affairs officials.

f. Senior Agency Official (SAO). The SAO will report any possible loss, compromise, or unauthorized disclosure of classified information to the Department of Transportation (DOT) Director of Security, M-40.

2. Inquiry, Investigation, and Corrective Actions.

a. CISM actions:

(1) Report the circumstances as soon as possible to their supporting Servicing Security Element (SSE);

(2) Begin a preliminary inquiry using the guidelines of paragraph 3; and

(3) Send the preliminary inquiry to their SSE within 3 working days of the incident.

b. SSE Actions:

(1) Report the incident to the CISPM;

(2) Provide advice and support to the CISM, who is conducting the preliminary inquiry; and

(3) Review the preliminary inquiry and forward it to the CISPM within ten working days of the incident.

c. CISPM Actions:

(1) Review the preliminary inquiry and decide if further investigation is necessary;

(2) If needed, coordinate with the appropriate SSE to conduct a formal investigation;

(3) Begin action to assess the potential damage to national security;

(4) If disciplinary action beyond a reprimand is possible, consult with the Office of Chief Counsel (AGC); and

(5) If a criminal violation is possible and we consider criminal prosecution, coordinate with the Department of Justice.

3. Preliminary Inquiry Guidelines. When a suspected loss or compromise of classified material occurs, the CISM will:

a. Search and document search steps. In cases of obvious loss, conduct a thorough search for the material and document the steps taken to find the material.

b. Seek help. Seek advice and support as needed from the supporting SSE.

c. Answer basic questions. Conduct an inquiry to answer these questions:

(1) *Who*? (Identify each individual involved, including management officials, and explain their involvement.)

(2) *What*? (Describe the information and material involved, what happened to it, and, if lost, what steps people took to find missing information.) The description must include:

- Classification and warning notices and control markings, if any;
- Subject or Title;

- Identification or serial numbers if any;
- Date of document;
- Originator;
- Original classification authority or Classified by;
- Declassification instructions and downgrading instructions, if any; and
- Number of pages or items of equipment involved.

(3) *When*?

- Date and time incident occurred (if known) and
- Date and time personnel discovered and reported the incident.

(4) *Where*?

- Complete identification of FAA facility: address, building and room number and
- For incidents involving unsecured and unattended security containers, the type of security container, the type of lock, and the security container's location in the room.

(5) *How* their organization disclosed, lost, or compromised the information?

Chapter 9. SAFEGUARDING CLASSIFIED INFORMATION

1. National and Department of Transportation (DOT) Policy.

a. Information Security Oversight Office (ISOO) Directive No. 1. Title 32 CFR Part 2001 Subpart D sets national policy for safeguarding classified information, and

b. Department of Transportation (DOT) Policy. DOT Order 1640.4, Classified National Security Information, sets DOT policy.

2. FAA Policy.

a. Restrictions on access. A person may have access to classified information when meeting these conditions:

(1) A Federal agency has made a favorable determination of eligibility for access and issued a security clearance to the person;

(2) The person has signed an approved nondisclosure agreement; and

(3) The person has a need-to-know specific classified information.

b. Exception to restrictions on access. EO 12958 allows exceptions to restrictions on access, and the Senior Agency Official (SAO) for the originating agency of the information may waive the restrictions.

c. Initial briefing. In conjunction with signing their Standard Form 312, Classified Information Nondisclosure Agreement, every FAA employee who has met the standards for access to classified information receives an initial briefing. (Page 6-1, paragraph 4a)

d. Agency control.

(1) Classified information remains under the control of the originating agency or its successor in function. The FAA may not disclose information originally classified by another agency without that agency's authorization.

(2) An official or employee leaving FAA service may not remove classified information from the FAA's control.

e. Proper authorization to remove. FAA personnel may not remove classified information from FAA property without proper authorization.

f. Dissemination outside executive branch. When sending classified information outside the executive branch, FAA personnel must ensure the receiver can protect the information in a manner equivalent to that provided by the executive branch.

g. National Security Systems. Consistent with laws, directives, and regulations, the SAO and AIO will set up uniform procedures to protect national security systems. These procedures will ensure that automated information systems, including networks and telecommunications systems, that collect, create, communicate, compute, disseminate, process, or store classified information have controls that:

(1) Prevent access by unauthorized people; and

(2) Ensure the integrity of the information.

h. Safeguarding measures. This order sets up compulsory measures to ensure the FAA uses, processes, stores, reproduces, transmits, and destroys classified information under protective conditions that prevent access by unauthorized people. The SAO in coordination with the DOT Director of Security, M-40, must approve alternative safeguarding measures.

i. Foreign Government Information (FGI).

(1) Holders of FGI information must safeguard it by this order; or

(2) By the protective standards of the treaty, agreement or other obligation with the government or international organization of governments that supplied the information. When a treaty, agreement or obligation applies to the information, the requirements at Appendix C may also apply to the extent mentioned by the treaty, agreement or obligation.

j. Classified information originated by another agency. Except as otherwise provided by statute, EO 12958, directives implementing EO 12958, or by direction of the President, the FAA will not disclose classified information originated by another agency outside the FAA without the written consent of the originating agency.

k. Protection and Classification Levels. The FAA affords classified information, regardless of its form, protection against loss or unauthorized disclosure equal to its classification level.

l. North Atlantic Treat Organization (NATO) classified information. U.S. Security Authority for NATO Instructions I-69 and I-70 apply to safeguarding and protecting North Atlantic Treaty Organization (NATO) classified information.

m. Emergency disclosure of classified information. In emergencies, the Administrator may approve emergency disclosure of classified information to personnel who are not eligible for access. Emergencies are situations where there is an imminent threat to life or in defense of the homeland. These conditions apply to emergency disclosures:

(1) Limit disclosure of classified information to the minimum to achieve the purpose;

(2) Limit the number of individuals who receive it;

(3) Transmit the classified information by the secure means of this chapter or by other means when time is of the essence;

(4) Specifically identify the classified information and provide the receiver instructions on how to safeguard it;

(5) In all but the most extraordinary circumstances, keep physical custody of the information with an approved Federal Government entity;

(6) Provide suitable briefings to recipients on their responsibilities not to disclose the information and get a signed nondisclosure agreement; and

(7) Within 72 hours of disclosing the information, or as the emergency allows, but no later then 30 days after the disclosure, provide the originating agency with this information:

- A description of the disclosed information;
- To whom we disclosed the information;
- How we disclosed and transmitted the information;
- Reason for the emergency disclosure;
- How the receiver is safeguarding the information; and
- A description of the briefings to the receivers and signed copies of nondisclosure agreements.

3. Responsibilities of Holders. Personnel who have access to classified information are responsible for:

- Protecting it from people without authorized access to that information. This includes securing it in approved equipment or facilities whenever it is not under the direct control of an authorized person;
- Safeguarding it as prescribed by this chapter; and
- Not communicating it over unsecured voice or data circuits, in public conveyances or places, or in any other manner that allows interception by unauthorized people.

4. Classified Visits. FAA Order 1600.74 addresses FAA policies and procedures for allowing visitors access to FAA facilities and information, including classified information. See FAA Orders 1600.69 and 1900.1 for other visit requirements.

5. Storage Standards.

FIGURE 9-1: FAA CLASSIFIED INFORMATION STORAGE REQUIREMENTS		
If your information is	Then you must store it within a closed area in	With one of these supplemental controls
Top Secret	A GSA approved Class 5 or 6 security container	• In a facility secured to the standards of FAA Order 1600.69 and a security container lock that meets Federal Specification FF-L-2740 (Note 1) • Continuous protection by cleared guard or duty personnel (Note 2) • Inspection every two hours of the security container by cleared guard or duty personnel • An acceptable intrusion detection system with a 15-minute response time by guard or duty personnel (Note 3)
Secret	1. The same manner as Top Secret information; or 2. A GSA approved Class 5 or 6 security container.	
Confidential	In the same manner as Top Secret or Secret information	
Notes: 1. As of September 30, 2005, the Kaba-Mas X-09 meets Federal Specification FF-L-2740. 2. Guard or duty personnel must be able to see the container or be able to see people approaching the container. 3. The regional Servicing Security Element decides acceptable intrusion detection systems.		

6. Standards for Security Equipment.

a. General Services Administration (GSA) standards. GSA publishes uniform standards, specifications and supply schedules for security equipment designed for secure storage and destruction of classified information. Whenever the FAA buys new security equipment, it must conform to GSA standards and specifications and to the maximum extent possible, be available through the Federal Supply System.

b. Servicing Security Element (SSE). Refer questions on standards for security equipment to your SSE.

c. Security containers.

(1) Procurement. Buy containers only from the items listed on the GSA Federal Supply Schedule. For lists of approved security containers see the DoD Lock Program Website – http://locks.nfesc.navy.mil.

(2) Combination lock standards:

(a) New buys. New combination locks must conform to Federal Specification FF-L-2740A for electromechanical locks. As of September 30, 2005, the Kaba-Mas X-09 lock was the only lock meeting this specification.

(b) Existing mechanical combination locks (UL Group 1). CISMs may continue using existing mechanical combination locks until they fail. If they fail, replace them with locks meeting Federal Specification FF-L-2740A.

(3) External Labels and Markings.

(a) Required forms and signs:

- SF 702, Security Container Check Sheet
- "OPEN – CLOSED" or "OPEN - LOCKED" signs
- "General Services Administration Approved Security Container" label. Only security containers that have passed all GSA testing to the requirements of a federal specification for security containers may bear this label. The manufacturer attaches the label to the container. A missing label is a sign that a container does not meet federal specification. It is also standard practice to remove the label if someone opens, repairs, or modifies an approved container in an unauthorized way.

(b) Labeling and marking prohibitions:

- Labels and markings revealing the classified contents of a container, and
- Priorities for emergency evacuation and destruction.

(c) For identification and inventory purposes security containers may bear labels and markings not about classified contents, such as, bar codes and inventory tags.

(4) Keep tops of security containers clear of unauthorized items. Storing, filing or placing items on top of security containers can lead to someone unintentionally leaving classified information unsecured or mixed with unclassified material.

(5) Container Records. CISMs must complete a Standard Form (SF) 700, Security Container Information) for each container storing classified information as follows:

- Complete part 1 and part 2A. Include the name and signature of the person changing the combination in item 9, part 1;
- Post part 1 on an inside wall of the container's locked drawer;
- Mark parts 2 and 2A with the highest classification of the material stored in the container;
- Detach part 2A and insert it into the SF 700 envelope;

- By paragraph 10b, page 9-9, wrap the envelope addressing it to your regional SSE; and
- Send it to your SSE by U.S. Postal Service Registered or Express mail or by courier.
- Do not keep written records of combinations in wallets, purses, briefcases, desk drawers, on calendars or notepads, or written "in code" or foreign languages. You may store written records combinations only in another GSA approved security container.

(6) Repair of Damaged Containers and Locks. Only GSA certified vendors may repair, inspect, and recertify damaged security containers and locks. To find a certified vendor in your area, contact your SSE.

(7) Changing combinations. Only personnel, who have a security clearance equal to the highest classification of the information stored in the security container, may change combinations. Change combinations:

- Whenever putting equipment into use;
- Whenever a person knowing the combination no longer needs access to it;
- Whenever a combination has been subject to possible unauthorized disclosure;
- Yearly; or
- When taking a container out of service. Set built-in combination locks to the standard combination 50-25-50 and set combination padlocks to the standard combination 10-20-30.

(8) Equipment out of service. When taking a security container out of service:

- Remove all classified information;
- Remove each container drawer and inspect the interior of the container to ensure no classified material remains; and
- Reset the built-in combination lock to the standard combination.

(9) Use only for storing classified information. To reduce risk that unauthorized persons have access to classified security containers, do not use these containers to store weapons or sensitive items such as funds, jewels, precious metals, or drugs.

7. Care During Working Hours.

a. Removing classified information from storage. When a user removes classified information from secure storage, they must:

(1) Keep it under constant surveillance and control by themselves or other authorized personnel;

(2) Place classified document cover sheets on the information:

- Standard Form (SF) 703 (Top Secret Cover Sheet),
- SF 704 (Secret Cover Sheet), or
- SF 705 (Confidential Cover Sheet).

(3) After they have served their purpose, immediately destroy all items such as drafts, carbons, notes, automated information storage media, typewriter and printer ribbons, plates, stencils, worksheets, and so on. See paragraph 11, page 9-11.

b. Standard Form 702 (Security Container Check Sheet). Visibly display SF 702 on each piece of equipment storing classified information. We use the SF 702 as follows:

(1) Each time a person opens or locks the container, they will record the date and time of opening or locking followed by their initials.

(2) When conducting security checks, the person conducting the check will record the date and time of the check followed by their initials.

(3) When filled out, keep it for at least 24 hours following the last entry.

c. Open and unattended security containers.

(1) A person discovering a security container open and unattended will:

- Keep the area under guard or surveillance.
- Contact one of the people listed on Part 1, SF 700 (Security Container Information), affixed inside the security container's lock drawer, the CISM, or the manager who is responsible for the space.

(2) The contacted individual will:

- If possible report personally to the location and
- Ensure that a person, who is knowledgeable of the container's contents, inventories those contents and checks the container and area around it for signs or evidence of tampering, theft, or compromise.
- If he or she suspects tampering, theft or compromise, contact their CISM and SSE for preliminary inquiry action.

(3) Change the combination by the procedures of paragraph 6c and lock the container.

8. End-of-Day Security Checks. CISMs must set up a system of security checks at the close of each working day to ensure their personnel properly secure classified material.

a. Standard Form 701 (Activity Security Checklist). We recommend SF 701 to record these checks.

b. After hours checks of desks and work spaces. CISMs may conduct after hours checks of desks and work spaces provided:

(1) They notify each employee affected by the local policy of procedures for conducting the checks to include policy for locking desks.

(2) Only appointed people conduct the checks for the *sole* purpose of detecting improperly secured classified information.

9. Reproduction. Because classified reproduction or copying pose unique risk, CISMs must set up local procedures to ensure that classified reproduction is:

a. Authorized.

(1) If an originator restricts reproduction, then get originator's written approval for reproduction.

(2) The Top Secret Control Officer must approve reproduction of Top Secret information.

(3) Classified Information Account Custodians of Security Control Points must approve reproduction of any classified material they control.

b. Limited and controlled. Managers must

(1) Limit the number of copies to meet needs or to help declassification reviews, and

(2) Control copies by the administrative control measures of Chapter 10.

c. Reproduced on authorized equipment.

(1) With their SSE's approval, CISMs will select suitable reproduction equipment. The equipment should not be the type that leaves latent images in the equipment or that holds images in electronic memory. This equipment may not be connected to networks.

(2) Certification and accreditation requirements for National Security Systems apply to equipment with electronic memory. If we cannot certify and accredit equipment with electronic memory, then we must protect it as a piece of classified equipment.

(3) CISMs will identify the equipment with a locally made, letter sized, sign that reads: "Approved for the Reproduction of Classified Information."

(4) CISMs will place the equipment in a closed area.

d. Reproduced by knowledgeable people. These people must:

(1) Know the local procedures for classified reproduction; and

(2) Be familiar with using the reproduction equipment.

10. Transmission.

a. Local procedures. CISMs must develop local procedures, see Appendix D, which ensure:

(1) Their organization sends and receives classified information in a manner which ensures they can detect evidence of tampering, and preclude unintentional access;

(2) Timely delivery to the intended recipient; and

(3) Authorized personnel are the recipients and they can properly store the classified information.

b. Wrapping and packaging classified information. When sending classified information outside a FAA facility:

(1) To conceal contents, enclose all classified information in two opaque layers, such as opaque envelopes, card board boxes, or wrapping paper.

(2) To detect tampering, apply tamper tape to seams.

(3) Clearly address the inner layer with the addresses of both the sender and the intended recipient, the highest classification of the contents, and any proper warning notices.

(4) Clearly address the outer layer with the organization titles and addresses of both the sender and intended recipient only. Ensure the outer enclosure has no markings suggesting classified contents. Identify recipients by name only as part of an attention line. The following exceptions apply:

- If the classified information is an internal part of a packable item of equipment, consider the outside shell or body as the inner enclosure provided it does not reveal classified information;
- If the classified information is an inaccessible internal part of a bulky item of equipment, consider the outside or body of the item a satisfactory enclosure provided observation of it does not reveal classified information;
- If the classified information is an item of equipment that is not reasonably packable and the shell or body is also classified, conceal it with an opaque enclosure that will hide all classified features;
- If using specialized shipping containers, including closed cargo transporters or diplomatic pouch, consider them outer enclosures; and
- When hand-carrying classified information outside a facility, a locked briefcase may serve as the outer enclosure.

(5) When mailing or shipping classified information to another FAA facility or organization, address it to the Security Control Point of the FAA facility or organization.

c. Couriers. When our personnel hand-carry classified information outside an FAA facility, they must have a courier appointment letter and a courier briefing. Couriers must keep the information under constant and continuous protection and make direct point-to-point delivery. See Appendix E for the format of a courier appointment letter and Appendix F for a courier briefing. The SAO may approve, as a substitute for a courier on direct flights, the use of specialized shipping containers that are:

(1) Of acceptable construction to provide evidence of forced entry;

(2) Secured with a high security padlock;

(3) Equipped with an electronic seal that would provide evidence of surreptitious entry; and

(4) Handled by the carrier in a manner to ensure the carrier protects the container until its delivery.

d. Transmission methods within and between the U.S., Puerto Rico, or a U.S. possession or Trust Territory.

(1) Top Secret. Under no circumstances may we use the U.S. Postal Service to transmit Top Secret information. You may transmit Top Secret information only by:

(a) Direct contact between authorized personnel;

(b) The Defense Courier Service or an authorized government agency courier service;

(c) An appointed courier or escort with Top Secret clearance; or

(d) Electronic means over approved communications systems.

(2) Secret. Only by:

(a) Any of the Top Secret methods;

(b) U.S. Postal Service Express Mail and U.S. Postal Service Registered Mail, providing you:

- Do not complete the Waiver of Signature and Indemnity block, item 11-B, on the U.S. Postal Service Express Mail Label; and
- Do not use street-side mail collection boxes.

(c) Cleared commercial carriers or cleared commercial messenger services.

(3) Confidential. By any of the methods for Secret information or by U.S. Postal Service Certified Mail.

e. Transmission methods to a U.S. Government facility located outside the U.S. When sending classified information to a U.S. Government facility outside the 50 states, the District of Columbia, the Commonwealth of Puerto Rico, or a U.S. possession or trust territory, use:

(1) Any of the methods mentioned above for Top Secret information or by the Department of State Courier Service.

(2) U.S. Registered Mail through U.S. Military Postal Service facilities to send Secret and Confidential information provided the information does not pass out of U.S. citizen control nor pass through a foreign postal system.

f. Transmission of U.S. classified information to foreign governments. The SAO must approve any transmission of classified information to foreign governments.

g. Receipt of classified information. Transmissions of Top Secret and Secret information require receipts from intended recipients.

11. Destruction. CISMs must set up destruction procedures that:

a. Preclude recognition and reconstruction. Ensures destruction of classified information to preclude recognition or reconstruction of the classified information by approved procedures and methods. The methods and equipment for destroying information to preclude recognition and reconstruction include burning, crosscut shredding, wet-pulping, melting, mutilation, chemical decomposition or pulverizing.

b. Crosscut shredder specification. Crosscut shredding is the FAA's primary method for destroying classified paper documents. The crosscut shredders we use to destroy classified paper documents must meet:

(1) National Security Agency (NSA) Specification 02-01, High Security Crosscut Paper Shredders – NSA publishes an Evaluated Products List for High Security Crosscut Paper Shredders that meets this specification; or

(2) Shred paper to a size not exceeding 5 square millimeters for 90% of the particles with no edge exceeding 5 millimeters in length.

c. Technical guidance. SSEs provide technical guidance on approved methods, equipment, and standards to destroy classified paper documents, electronic media, and electronic processing equipment components.

12. Classified Discussions and Meetings. Anyone who discusses classified information must ensure that unauthorized personnel, *particularly uncleared personnel*, do not overhear the discussion. These precautions apply to classified discussions and meetings:

a. Public places. Never discuss classified information in public areas, conveyances, or rooms where you have no control over bordering areas, for example, hotel and rest rooms. Many rooms, including those in government buildings, have ducts and vents that conduct sound to unintended areas.

b. Infrequent discussions and meetings. If you discuss classified information infrequently – two or three times a month – you may use an office if you can close the door and no one in adjoining offices can hear your conversation.

c. Frequent discussions and meetings. Spaces where you often discuss classified information are at risk for eavesdropping. You must designate these spaces "closed area."

d. Secure telephones. You may not use unsecure telephones to discuss classified information. You must use Secure Telephone Equipment (STE) or a Secure Telephone Unit, third generation (STU-III) when you need to discuss classified information over a telephone. See Appendix H – Using Secure Telephones.

13. Special Access Programs (SAP).

a. Some FAA elements and personnel participate in SAPs of other U.S. Government agencies. These elements and personnel must coordinate their participation with ASH-1. This coordination insures the organization identifies special security requirements pertaining to the SAP, such as special clearances, secure telecommunications equipment, and secure storage. Coordination also insures the FAA element or employee has executive level approval for participation.

b. AEO-300, National Security Coordination Division, is the point of contact for outside agencies seeking FAA support in sensitive and classified law enforcement, military, intelligence, or other national security or homeland security activities.

14. Telecommunications, Automated Information Systems and Network Security.

a. Communications Security (COMSEC). FAA Order 1600.8 discusses FAA policies and procedures and assigns responsibilities to comply with national COMSEC policy.

b. National Security Systems. In coordination with AIO-1, the SAO will set up a program to ensure the FAA protects classified information electronically accessed, processed, stored or transmitted. This program will follow applicable national policy issuances identified in the Index of Issuances of the Committee on National Security Systems (CNSS). The index and other CNSS references are at http://www.cnss.gov.

15. Technical Security Countermeasures. Technical surveillance countermeasures (TSCM) are techniques and measures to detect and neutralize a wide variety of hostile penetration technologies designed to identify unauthorized access to information. (FAA Order 1600.12)

Chapter 10. ADMINISTRATIVE CONTROL MEASURES

1. Purpose. By EO 12958 and 32 Code of Federal Regulations Part 2001.44, we must have control measures to ensure that only authorized people have access to our classified information. Within the FAA, we use technical, physical, personnel, and administrative control measures to achieve this end. This chapter sets up our *administrative control measures*, including accounting measures. Through administrative control measures, we can:

- Limit and control access;
- Trace movement of classified information and material;
- Identify anyone who has access;
- Find and retrieve documents quickly;
- Detect the loss of information or material; and
- Prevent excessive production and reproduction of documents.

2. Administrative Control Measures for Managers:

FIGURE 10-1 MANAGER'S ADMINISTRATIVE CONTROL MEASURES

If your office, activity, or facility	*Then you must*
Uses, handles, stores, or processes classified information	• Appoint an appropriately cleared Classified Information Security Manager (CISM) • Select closed areas where the organization will use, handle, or process classified information • Use FAA Form 1600.83 ► to set up a Security Control Point (SCP) overseen by the CISM and ► to appoint an appropriately cleared Classified Information Account Custodian (CIAC) and Alternate Information Account Custodian (ACIAC) to run the SCP • Coordinate with your Security Servicing Element (SSE) for CISM, CIAC, and ACIAC training before they assume their duties • Ensure the performance plans of CISMs, CIACs, and ACIACs list their duties as critical outcomes
Stores classified information in multiple locations	Use FAA Form 1600.83 to set up Document Control Stations (DCS) and to appoint CIACs and ACIACs to run them
Uses, handles or processes Top Secret information	• Use FAA Form 1600.83 to appoint a TOP SECRET Control Officer (TSCO) and • Ensure the TSCO sets up TS accounting measures of this chapter
Stores Secret information	Ensure the CISM and CIAC set up the accounting measures of this chapter
Uses Communications Security (COMSEC) materials	Follow the procedures of FAA Order 1600.8, Communications Security (COMSEC) and Secure Voice

3. Closed Areas. These are spaces where an organization processes, handles, transmits, or stores classified information on a regular basis. Closed areas include, but are not limited to, Security Control Points, Document Control Stations, and spaces where the organization stores, reproduces, or processes classified information. Closed area protective measures:

a. Physical measures:

(1) Physical barriers – walls, ceiling, and doors with FAA standard "Best" locks – must separate a closed area from adjacent spaces. These barriers will control physical, aural, or visual access into the closed area.

(2) Appropriately cleared employees or monitored access control systems will control access to closed areas. Regional SSEs must approve access control systems.

(3) If the organization stores bulky classified material, that when unattended cannot be stored in a GSA approved security container, the closed area must meet the construction standards for open storage of Title 32 CFR § 2001.52.

b. Administrative measures for closed areas:

(1) Managers will restrict unescorted access to appropriately cleared members of their staff.

(2) To prevent inadvertent or unauthorized disclosure of classified information, appropriately cleared employees must escort uncleared persons and visitors while these persons are in a closed area.

4. Security Control Points. Each FAA organization or facility that handles classified information must set up a SCP that performs under supervision of a CISM. We use FAA Form 1600.83 to set up SCPs and to appoint SCP operators: CIACs and ACIACs. Before starting duties, CIACs and ACIACs must have final secret clearances. SCP functions:

a. Process classified material. Process all incoming and outgoing classified material for the organization or facility;

b. Account for secret materials. Assign document control numbers to all Secret material received by the office or activity and keep accountability records for Secret information;

c. Verify security clearances. Verify the security clearance of each person who has access to the organization's classified information and ensure they can provide proper safeguards before transferring classified information to their control;

d. Incoming classified material.

(1) On opening any mail or shipment containing classified material, match the contents of the package with any enclosed receipt; and

(2) If the mail or shipment has a return receipt, sign and return the receipt to the sender;

e. Outgoing classified material.

(1) For outgoing classified material select suitable secure methods of transmission consistent with this order; and

(2) For Secret material get receipts;

f. Destruction. Destroy or arrange destruction of classified material as directed by this order; and

g. Accountability records. Keep accountability records for Secret information.

5. Classified Information Account Custodian Duties:

a. Protective focal point. Serve as the focal point for protecting classified information at their SCP;

b. Apply suitable control measures. Apply suitable technical, physical, personnel, and administrative control measures to their account;

c. Report statistical data. As needed, develop and report statistical data to their SSE;

d. Inventory. Conduct yearly inventories of Secret documents;

e. Access lists. Keep a list of cleared people and their clearance level, who have access to SCP or DCS classified information; and

f. Report and investigate. Take immediate action to report and investigate suspected compromises of classified information and suspected security violations.

6. Top Secret Control Officer. Managers of organizations and facilities that handle Top Secret information must appoint in writing a TSCO and, if needed, an alternate TSCO. Before a TSCO assumes duties, the SSE must approve their appointment, and they must have a final Top Secret Clearance. The TSCO may be the CISM or CIAC. TSCO duties and functions:

a. Control access. Ensure only properly cleared people have access;

b. Safeguard. Receive, keep permanent custody of, account for, dispatch, and protect all Top Secret material for the office, activity, or facility;

c. Separate storage. Store Top Secret material separately from other classified material to ensure that only properly cleared personnel have access to it;

d. Accountability records. Keep the accountability records and controls required by this appendix;

e. Top Secret Disclosure Record. Affix a Top Secret Disclosure Record, FAA Form 1600.81, to each TS document. This record reflects the document title, the name of all individuals who have had access to the document, including aural disclosures, and the dates of such access;

f. Continuous receipt system. Ensure a continuous receipt system, regardless of how brief the period of custody, for the internal and external transfer of TS information;

g. Accounting controls. Number TS documents in series and ensure distribution records, receipts, and accountability records list the copy number as part of the document identification; and

h. Inventories. Conduct semiannual inventories of TS material in June and December of each year and report the results of those inventories to their SSE.

7. Document Control Stations. If organizations or facilities store classified material at multiple locations, they may set up DCSs, as needed. DCSs run under the supervision of the CISM and the CIAC of the main SCP. We use FAA Form 1600.83 to set up a DCS and to appoint the CIAC and ACIACs to run it. DCS functions:

a. Store classified information. Receive all Secret and Confidential materials that flow into or out of the organization or facility the DCS supports. TSCOs must handle Top Secret information.

b. Records. Keep FAA Form 1600.35, Classified Document Register, for Secret material handled by the DCS.

c. Control access. Ensure only properly cleared personnel have access to classified information and that they are familiar with the procedures for properly safeguarding classified material.

8. Accounting Controls.

a. Secret information. The SCP must set up and keep current FAA Form 1600.35, Classified Document Register. CIACs use this register when their SCP or DCS receives, creates, transfers, reproduces, or destroys Secret material.

b. Communications security (COMSEC), Special Intelligence, Registered Publication Systems, Restricted Data, National Security Council (NSC) Intelligence Information, and other unique material. Classified materials in these categories are accountable under other control systems.

(1) FAA Order 1600.8, Communication Security (COMSEC) and Secure Voice, addresses our policy and procedures for protecting COMSEC information to include appointing COMSEC custodians. The Committee on National Security Systems (CNSS) issues COMSEC related classified documents that we control under this order. You'll find these documents listed in CNSS 4009, Index of National Security System Issuances.

(2) NSC information is classified information in any document prepared by or used by the NSC, its interagency groups, or its associated committees and groups. NSC information also includes deliberations of the NSC, its interagency groups, or its associated committees or groups. The DOT holds the number of people having access to NSC information to the minimum consistent with efficient operations of the NSC system, and strictly controls document dissemination and reproduction. The NSC prepares and distributes a special cover sheet for all NSC documents.

c. Classified material hand carried to or from an FAA organization or facility. Anyone who receives classified material from a visitor, or who brings classified material back to their organization because of a visit to another organization, must immediately have the material processed by the SCP. The TSCO or Alternate TSCO must process Top Secret material. Similarly, personnel who release Secret material directly to an authorized person or to another activity because of a visit must get a receipt, Classified Material Record, FAA Form 1600.82 for the material. FAA personnel must coordinate with their CIAC or ACIAC, in the CIAC's absence, before any such transfer. FAA personnel returning to their office with classified material must properly mark and protect the classified material while in transit.

d. Confidential information. We do not require accountability records for Confidential material. However, the SCP or DCS must handle all incoming and outgoing Confidential material to ensure we comply with marking, packaging procedures, declassification guidance, and other security requirements.

9. Inventories.

a. Frequency. TSCOs and CIACs must conduct inventories and report inventory results through management channels to their SSE at these frequencies:

(1) Top Secret. Semi-annually in June and December of each year.

(2) Secret. Yearly in December of each year.

b. TSCO and CIAC inventory procedures:

(1) Sight each accountable item or evidence of its proper disposition, for example, transfer receipt, destruction certificate, or record of downgrading or declassification;

(2) Physically inventory the entire contents of security containers to ensure that all Top Secret and Secret material is in the accountability system;

(3) Destroy classified documents the activity or office no longer needs; and

(4) Inspect security containers to ensure each container:

- Is GSA approved and is serviceable and properly maintained;
- Has the proper combination lock and the lock works properly;
- Has had its combination changed as required by this order;
- Has the forms required by this order.

10. Classified Working Papers. Working papers are documents, including drafts, notes, and photographs that we collect or create to develop and prepare a finished classified document.

a. Disclosure within an organization or facility. Classifiers may release Secret and Confidential working papers within an organization or facility for review and coordination without processing the working paper through the SCP or DCS under these conditions:

(1) The person responsible for the working papers ensures the recipients have the proper security clearance, need to know, and ability to store the information properly.

(2) The person responsible for the working paper gets a receipt, FAA Form 1600.82, for Secret working papers. The recipient must sign the receipt and the CIAC keeps it with a copy to the recipient.

(3) The recipient must return the working paper to the releasing office within 30 days or enter the working paper into the accounting records of the SCP or DCS.

b. Marking working papers. Originators of working papers must:

(1) Date them when created;

(2) Mark the document with the highest classification of any information it contains;

(3) Mark the document with declassification instructions;

(4) Protect the document at its assigned classification level;

(5) Destroy the document by means approved by the SCP or DCS when no longer needed;

(6) Use a document cover sheet (SF-703, SF-704, or SF-705) to protect working papers from inadvertent disclosure;

(7) Mark folders for filing working papers at the top and bottom, front and back, with the highest classification the material stored within the folder; and

(8) Account for, control, and mark as a finished document when the working paper is 180 days old or the originator releases it outside the organization or facility.

11. Retention of Classified Accountability Records. See Chapter 4, FAA Order 1350.15C.

FIGURE 10-2, RETAINING CLASSIFIED ACCOUNTABILITY RECORDS

If your SCP has these records	***Then you may***
Registers showing accountability for Top Secret documents reflecting receipt, dispatch, or destruction of the documents.	*Destroy* 5 years after the documents shown on forms are downgraded, transferred, or destroyed
Forms accompanying documents to ensure continuing control, showing names of anyone handling the documents, intraoffice routing, and comparable data.	Destroy when related document is downgraded, transferred, or destroyed
Records about information or material classified confidential	Destroy 2 years after final disposition of related material
Records documenting the receipt and issuance of classified documents	Destroy when 2 years old
Certificates about the destruction of classified documents	Destroy when 2 years old
Forms, ledgers, or registers used to show identity, internal routing, and final disposition of Secret and Confidential documents	Destroy when 2 years old
Requests and authorizations for individuals to have access to classified files	Destroy 2 years after authorization expires

Chapter 11: ADMINISTRATIVE INFORMATION

1. Distribution of This Order. Distribute this order to:

- Branch level and above at the Washington and regional headquarters;
- Branch level and above at the Mike Monroney Aeronautical Center and the FAA Technical Center;
- Overseas area offices; and
- All field facilities.
- It is also electronically available at http://dmis.faa.gov.

2. Authority to Change This Order.

a. Changes. The Assistant Administrator for Security and Hazardous Materials, ASH-1, issues changes which do not change FAA policy, delegation of authority, assignment of responsibility, or have a significant impact on resources.

b. Supplements. In coordination with ASH-1, lines of business and regional Servicing Security Elements may supplement this order to fulfill it within their respective areas of responsibility.

3. Definitions. Appendix A

4. Related Publications. Appendix G.

5. Forms and Reports. Appendix B.

6. For More Information. Your Security Servicing Element (SSE) can answer any questions about this order. In regions your SSE is the Security and Hazardous Materials Division, AXX-700, and at the Washington Headquarters, the SSE is the Office of Internal Security and Investigations, AIN-1.

APPENDIX A. DEFINITIONS

Access means the ability or opportunity to gain knowledge of classified information.

Accreditation means a formal declaration by a Designated Approving Authority (DAA) that an automated information system may perform in a particular security mode using a prescribed set of safeguards.

Agency means any "Executive agency," as defined in Title 5 U.S.C. 105; any "Military department" as defined in 5 Title U.S.C. 102; and any other entity within the executive branch that possesses classified information.

Authorized person means a person who:

- Has a favorable determination of eligibility for access to classified information,
- Has signed an approved nondisclosure agreement, and
- Has a need-to-know for the specific classified information in performing official duties.

Automated information system means an assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

Automatic declassification means declassifying information based solely on:

- The occurrence of a specific date or event as determined by the original classification authority; or
- The expiration of a maximum time frame for duration of classification set up under EO 12958.

Certification means a comprehensive evaluation of the technical and non-technical security features of a system and other safeguards, made in support of the accreditation process. Certification establishes the extent to which a particular design and implementation meets a set of specific security requirements.

Classification means the act or process by which information is determined to be classified information.

Classification guidance means any instruction or source that prescribes the classification of specific information.

Classification guide means a documentary form of classification guidance issued by an original classification authority. A classification guide identifies the elements of information about a specific subject that we must classify and establishes the level and duration of classification for each such element.

Classified Information Account Custodian (CIAC) means an employee who operates a Security Control Point (SCP).

Classified Information Security Manager (CISM) means the employee who oversees the day-to-day management of an organization's program for safeguarding classified information.

Classified Information Security Program Manager (CISPM) means manager who oversees day-to-day management of the FAA's program for safeguarding classified information.

Classified national security information or *classified information* means information that has been determined by EO 12958 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

Cleared commercial carrier means a carrier that is authorized by law, regulatory body, or regulation, to transport SECRET and CONFIDENTIAL material and has been granted an SECRET facility clearance under the National Industrial Security Program.

Closed area means an area where the FAA processes, handles, transmits, or stores classified information on a regular basis. Management:

- May designate a closed area only for safeguarding classified information and for no other purposes;
- Will limit unescorted access to closed areas to cleared personnel, who have a valid need-to-know the information contained in the area;
- Identify closed areas by affixing closed area signs to accessible perimeter surfaces; and
- Secure unattended closed areas.

Compilation means an aggregation of preexisting unclassified items of information.

Compromise means the unauthorized disclosure of classified information to persons who do not have a valid clearance, authorized access, or a need-to-know. A possible compromise can occur when we fail to properly safeguard classified information.

Confidential source means any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters about the national security. Confidential sources have the expectation the United States will hold their information or relationship, or both, in confidence.

Damage assessment means a multidisciplinary analysis to determine the effect of a compromise of classified information on the national security.

Damage to the national security means harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information. Damage to the national security considers such aspects of the information as the sensitivity, value, utility, and provenance of that information.

Declassification means the authorized change in the status of information from classified to unclassified information.

Declassification authority means:

- The official who authorized the original classification, if that official is still serving in the same position;
- The originator's current successor in function;
- A supervisory official of either; or
- Officials delegated declassification authority in writing by the agency head or the senior agency official.

Declassification guide means written instructions issued by a declassification authority that describes the elements of information about a specific subject that you may declassify and the elements that must remain classified.

Derivative classification means the act of incorporating, paraphrasing, restating, or generating in new form already classified information, and marking the newly developed material consistent with the classification markings of the source information. Derivative classification includes classifying information based on classification guidance. Duplication or reproduction of existing classified information is not derivative classification.

Designated Approving Authority (DAA) means the official with the authority to formally assume the responsibility for operating a system at an acceptable level of risk.

Document means any recorded information, regardless of the nature of the medium or the method or circumstances of recording.

Document Control Station (DCS) means an additional place where an organization stores classified information when the organization must store classified information at multiple locations. The DCS work under the supervision of the main SCP.

Downgrading means a determination by a declassification authority that information classified and safeguarded at a specified level must be classified and safeguarded at a lower level.

Employee means a person, other than the President and Vice President,

- Employed by, detailed or assigned to, an agency, including members of the Armed Forces;
- An expert or consultant to an agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of an agency, including all subcontractors;
- A personal services contractor; or
- Any other category of person who acts for or on behalf of an agency as determined by the appropriate agency head.

File series means file units or documents arranged according to a filing system or kept together because they:

- Relate to a particular subject or function,
- Result from the same activity,
- Document a specific kind of transaction,
- Take a particular physical form, or
- Have some other relationship arising out of their creation, receipt, or use, such as restrictions on access or use.

Foreign government information means:

a. Information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element of it. Foreign governments provide the information with the expectation that we will hold the information, the source of the information, or both, in confidence.

b. Information produced by the United States Government under or because of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element of it. The arrangement requires we hold the information, the arrangement, or both, in confidence.

c. Information received and treated as "foreign government information" under the terms of a predecessor order to EO 12958.

Information means any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics that is owned by produced by or for, or is under the control of the United States Government. *Control* means the authority of the agency that originates information, or its successor in function, to regulate access to the information.

Information systems security (INFOSEC) means protecting information systems, and information handled by such systems, against:

- Unauthorized access,
- Modification of information, whether in storage, processing, or transit, and
- Denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.

Information systems security manager (ISSM) means the individual responsible for a program, organization, system, or enclave’s information assurance program.

Infraction means any knowing, willful, or negligent action contrary to EO 12958 or its implementing directives that does not constitute a “violation,” as defined below.

Integral file block means a distinct component of a file series that should be maintained as a separate unit to ensure the integrity of the records. An integral file block may consist of a set of records covering either a specific topic or time period such as presidential administration.

Integrity means the state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.

Intrusion detection system (IDS) means the combination of components, including sensors, control units, transmission lines, and monitor units, integrated to initiate alarm signals for intrusion threats.

Loss of classified information occurs when we cannot physically find or account for classified information, for example, lost during transmission.

Mandatory declassification review means the review for declassification of classified information in response to a request for declassification under section 3.5 of EO 12958.

Multiple sources mean two or more source documents, classification guides, or a combination of both.

National Information Assurance Certification and Accreditation Process (NIACAP) means a standard national process to certify and accredit national security systems.

National security means the national defense or foreign relations of the United States.

National Security Systems (NSS) means telecommunications and automated information systems used by the U.S. Government, its contractors, or its agents, that contain classified information or as set forth in Title 10 U.S.C. Section 2315 that involves:

- Intelligence activities,
- Cryptologic activities related to national security,
- Command and control of military forces,
- Equipment that is an integral part of a weapon or weapon system,
- Equipment that is critical to the direct fulfillment of military or intelligence missions, or
- Systems that store, process, or communicates classified information.

Need for access means a determination that an employee needs access to *a particular level* of classified information to perform or assist in a lawful and authorized governmental function.

Need-to-know means a determination made by an authorized holder of classified information that a prospective recipient needs access to *specific* classified information to perform or assist in a lawful and authorized governmental function.

Network means a system of two or more computers that can exchange data or information.

Open storage area means an area, built to the standards of 32 CFR Subpart D § 2001.52 and approved by the SAO for open storage of classified information.

Original classification means an initial determination that information requires protection against unauthorized disclosure in the interests of national security.

Original classification authority (OCA) means an individual authorized in writing, either by the President, the Vice President in the performance of executive duties, or by agency heads or other officials designated by the President, to classify information in the first instance. These individuals include:

- The official who authorized the original classification, if that official is still serving in the same position;
- The originator's current successor in function;
- A supervisory official of either; or
- The senior agency official.

Originating Agency's Determination Required or its acronym *"OADR "* mean a marking indicating an indefinite duration of classification under a predecessor executive order to EO 12958.

Overseas Security Policy Board (OSPB) means the Board set up by the President to consider, develop, coordinate and promote policies, standards, and agreements on overseas security operations, programs and projects. OSPB policies, standards, and agreements affect all United States Government agencies under the authority of a Chief of Mission.

Permanently valuable information or permanent historical value refers to information contained in:

- Records that have been accessioned into the National Archives of the United States;
- Records that have been scheduled as permanent under a records retention schedule approved by the National Archives and Records Administration (NARA); and
- Presidential historical materials, presidential records or donated historical materials found in the National Archives of the United States, a presidential library, or any other approved repository.

Preliminary inquiry means the initial process to determine the facts surrounding a possible loss or compromise of classified information.

Records mean the records of an agency and Presidential papers or Presidential records, as those terms are defined in Title 44, United States Code. Records include those created or maintained by a government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency’s control under the terms of the contract, license, certificate, or grant.

Records having permanent historical value means Presidential papers or Presidential records and the records of an agency the Archivist has determined should be maintained permanently under title 44, United States Code.

Records management means the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with records creation, records maintenance and use, and records disposition. Records management achieves adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations.

Redaction means the permanent removal of classified information from copies of a document so that recovery of classified information is not possible using any known techniques or analysis.

Safeguarding means prescribed measures and controls to protect classified information.

Security control point (SCP) means the place set up by an organization to control and safeguard incoming and outgoing classified material. The organization's CIAC, under the supervision of the organization's CISM, operates the SCP.

Security-in-depth means a determination by the SAO that a facility's security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the facility. Examples include, but are not limited to,

- Use of perimeter fences, employee and visitor access controls, use of an Intrusion Detection System (IDS), random guard patrols throughout the facility during nonworking hours, closed-circuit video monitoring;
- Or other safeguards that mitigate the vulnerability of open storage areas without alarms and security storage cabinets during nonworking hours.

Self-inspection or inspection means the internal review and evaluation of individual agency activities and the agency for implementing the program established under EO 12958.

Senior agency official (SAO) means the official designated by the agency head under section 5.4(d) of EO 12958 to direct and administer the program under which the agency classifies, safeguards, and declassifies information.

Sensitive Compartmented Information (SCI) means classified information about or derived from intelligence sources, methods, or analytical processes that must be handled with formal access control systems established by the Director of Central Intelligence.

Source document means an existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

Special access program (SAP) means any program set up to control access and distribution and to provide special protection for particularly sensitive classified information beyond the

requirements of this order. A SAP can only be set up by a SAO who has been delegated SAP authority by EO 12958.

Systematic declassification review means the review for declassification of classified information contained in records that have been determined by the Archivist to have permanent historical value under Title 44, United States Code.

Telecommunications means the preparation, transmission, or communication of information by electronic means.

Transferred records, by EO 12958, when classified records are transferred with a transfer of functions, the receiving agency is deemed to be the originating agency for the purposes of EO 12958. This provision of the EO affects classified records associated with the functions the FAA transferred to the Transportation Security Administration (TSA). When the FAA transferred security functions and their related classified records to TSA, TSA became the originating agency for those records.

Transnational terrorism means threats from activities conducted by individuals or groups that involve international terrorism, narcotrafficking, weapons of mass destruction and their delivery systems that threaten the national security of the United States.

Unauthorized disclosure means a communication or physical transfer of classified information to an unauthorized recipient.

Vault means an area approved by the SAO which is designed and constructed of masonry units or steel lined construction to provide protection against forced entry. A modular vault approved by the General Services Administration (GSA) may be used instead of an open storage area as prescribed by 32 CFR Subpart D § 2001.52. Vaults must have a GSA-approved vault door and lock.

Violation means:

- Any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information;
- Any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of EO 12958 or its implementing directives; or
- Any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of EO 12958.

Visitor, for this order, visitor means any person who is not attached to, employed by, or on temporary duty order to the FAA.

Weapons of mass destruction means chemical, biological, radiological, and nuclear weapons.

APPENDIX B. FORMS

The FAA uses these forms to manage classified information. The Federal Supply System supplies forms that have a National Stock Number (NSN). Forms marked by an asterisk are available online. Refer questions about these forms to your Servicing Security Element.

SF-311 Agency Security Classification Management Program Data*
The SF-311 is a standard data collection form for information about each agency's security classification program. The FAA sends it yearly to the Information Security Oversight Office through the DOT. NSN: NA

SF-312 Classified Information Nondisclosure Agreement*
The SF-312 is a non-disclosure agreement that all clear people must sign as a condition of access to classified information. NSN: 7540-01-280-5499

SF-700 Security Container Information
The SF-700 identifies individuals to contact if someone finds a security container open and unattended. The form also includes the means to preserve a current record of the security container's combination and an envelope to send the information to the right agency official. NSN: 7540-01-214-5372

SF-701 Activity Security Checklist*
The SF-701 provides a systematic means to make a thorough end-of-day security inspection for a particular work area and to allow for employee accountability when discovering irregularities. NSN: 7540-01-213-7899

SF-702 Security Container Check Sheet*
The SF-702 provides a record of the names and times that people have opened, closed or checked a particular container that holds classified information. NSN: 7540-01-213-7900

SF-703 Top Secret Cover Sheet
The SF-703 attaches to TOP Secret Classified documents. It protects the document from unintentional disclosure and alerts observers to its sensitivity. NSN: 7540-01-213-7901

SF-704 Secret Cover Sheet
The SF-704 attaches to Secret Classified documents. It protects the document from unintentional disclosure and alerts observers to its sensitivity. NSN: 7540-01-213-7902

SF-705 Confidential Cover Sheet
The SF-705 attaches to Confidential Classified documents. It protects the document from unintentional disclosure and alerts observers to its sensitivity. NSN: 7540-01-213-7903

SF-706 Top Secret Label
The SF-706 is a self-adhesive label that affixes to automated data processing media and other media containing Top Secret information to identify and protect the media.
NSN: 7540-01-207-5536

SF-707 Secret Label
The SF-707 is a self-adhesive label that affixes to automated data processing media and other media containing Secret information to identify and protect the media. NSN:7540-01-207-5537

SF-708 Confidential Label
The SF-708 is a self-adhesive label that affixes to automated data processing media and other media containing Confidential information to identify and protect the media.
NSN: 7540-01-207-5538

SF-709 Classified Label
The SF-709 is a self-adhesive label that affixes to automated data processing media and other media containing classified information to identify and protect the media until a determination by the classifier of the specific classification level of the information. NSN: 7540-01-207-5540

SF-710 Unclassified Label
SF 710 is a self-adhesive label that affixes to automated data processing media and other media containing unclassified information to identify and protect the media. In a mixed processing environment, the SF 710 functions to distinguish classified from unclassified media.
NSN: 7540-01-207-5540

SF-711 Data Descriptor Label
The SF-711 is a self-adhesive label that affixes to automated data processing and other media to identify added safeguards or controls about the classified information stored in the media.
NSN: 7540-01-207-5541

Optional Form (OF) 89, Maintenance Record for Security Containers/Vault Doors *
NSN: NA

Department of Defense (DD) Form 254, Department of Defense Contract Security Classification Specification
The Federal Acquisition Regulation (FAR) requires a DD Form 254 for each classified contract. The DD Form 254 provides the contractor or subcontractor the security requirements and the classification guidance necessary to perform on a classified contract. NSN: NA

FORM DOT F 1630.5, Visit Clearance
This form functions to verify clearances of FAA employees when the employees visit another Federal agency. FAA Order 1600.74

FAA Form 1600-35, Classified Material Register**
This form is a Microsoft Excel spreadsheet. Classified Information Account Custodians use it to account for Secret classified materials. Page D-4 shows this form.

FAA Form 1600-49, Reproduction Notice**
This is a Microsoft Word document. Classified Information Security Managers and Classified Information Account Custodians use it to identify approved equipment for reproducing classified information. Page D-5 shows this form.

FAA Form 1600-81, Top Secret Disclosure Record**
This is a Microsoft Word document. Top Secret Control Officers use to manage Top Secret information. Page D-6 shows this form.

FAA Form 1600-82, Classified Material Record**
This is a Microsoft Word document. Classified Information Account Custodians use it to manage their Secret information. Page D-7 shows this form.

FAA Form 1600-83, Security Control Point and Document Control Station Authorization**
This is a Microsoft Word document. The FAA uses this form to set up Security Control Points and Document Control Stations and to appoint the officials to operate them. Page D-8 shows this form.

Magnetic OPEN-CLOSED Reversible Sign. This sign is a visible reminder that a security container is open. It's available through various vendors. Hamilton Products Group, phone 800-876-6066, sells them under Product Code Number: 1460.

***** Forms available on line at http://www.gsa.gov/forms
** Forms available through the FAA Electronic Document System (FEDS)

Classified Material Register							
Control Number	**Subject or Description**	**Material Date**	**Date In**	**Classified by**	**Declassify or downgrade on**	**# of copies**	**Disposition**

FAA FORM 1600.35 (Dec 05)

TOP SECRET DISCLOSURE RECORD	TOP SECRET CONTROL NUMBER

NOTE: Each person who receives, or reads the attached document must complete, sign, and date Part 4

TOP SECRET

PART 1 - DOCUMENT DESCRIPTION

MEMO, LETTER, MESSAGE, ETC	DATE	DATE RECEIVED
SUBJECT		
ORIGINATOR	ADDRESS	

PART 2 - DOCUMENT INFORMATION

	ACTION COPY		INFORMATION COPY	COPY NO. OF COPIES

TOP SECRET CONTROL OFFICER'S SIGNATURE	ROUTING SYMBOL	DATE

PART 3 - TO BE COMPLETED BY EACH PERSON WHO HAS ACCESS TO THE ATTACHED DOCUMENT

NAME *(Signature)*	ORG.	DATE	NAME (*Signature)*	ORG.	DATE

PART 4 - DISPOSITION CONTROL

The Top Secret Control Officer completes this part when transferring the document outside the FAA or when downgrading, declassifying, destroying, or retiring the document. When completed, the Top Secret Control Officer will retain this record for four years.

☐	TRANSFERRED *(Outside FAA)*	ADDRESSEE	RECEIPT *(Attach)* ☐
☐	DOWNGRADED OR DECLASSIFIED	DATE	NEW CLASSIFICATION
☐	DESTROYED	☐ RETIRED	SIGNATURE OF WITNESS

TOP SECRET CONTROL OFFICER SIGNATURE	ORG.	DATE

FAA Form 1600.81 (Dec 05)

Federal Aviation Administration CLASSIFIED MATERIAL RECORD	**DATE RECEIVED**	**CONTROL NO.**

SECTION A – INFORMATION IDENTIFICATION			
CLASSIFICATION	☐ **TOP SECRET**	☐ **SECRET**	☐**CONFIDENTIAL**

ITEMS:

CLASSIFIED BY:
REASON:
DECLASSIFY ON:

SECTION B – INTERNAL ROUTING RECORD			
FROM (ROUTING SYMBOL)	**TO** (ROUTING SYMBOL)	**RECEIVED BY** (SIGNATURE)	**DATE**

SECTION C – DESTRUCTION RECORD			
Destroyed by Signature	Routing Symbol	Witnessed by Signature	Routing Symbol
TYPED OR PRINTED NAME	DATE	TYPED OR PRINTED NAME	DATE

SECTION D – EXTERNAL ROUTING RECEIPT	
FROM:	**TO:**

MATERIAL IDENTIFIED ABOVE RECEIVED BY	
SIGNATURE:	
TYPED OR PRINTED NAME:	
RECEIVING OFFICE:	**DATE:**

FAA FORM 1600.82 (Dec 05)

SECURITY CONTROL POINT AND DOCUMENT CONTROL STATION AUTHORIZATION

THRU: Personnel Security Officer:

TO: Office of Internal Security, AIN-1

Part 1 – Requestor Information

Date	Line of Business or Office	Division or Branch and Routing Symbol

By FAA Order 1600.2, request authority to set up a Security Control Point (SCP) or Document Control Station (DCS) and to appoint the officials to manage and operate them. Officials: Classified Information Security Manager (CISM), Top Secret Control Officer (TSCO), Classified Information Account Custodian (CIAC), and Alternate Classified Information Account Custodian (ACIAC).

Type Authorization SCP ☐ DCS ☐

Officials	Name	Phone	Routing Symbol	Clearance		
				TS	S	C
CISM				☐	☐	☐
TSCO				☐	☐	☐
CIAC				☐	☐	☐
ACIAC				☐	☐	☐

Information About This Request

Check the levels of classified information you will handle?	TS	☐	S	☐	C	☐
Do you have a GSA approved security container?	Yes	☐	No	☐		
If yes to above, what type of lock is installed on this container?						
Does your organization create classified documents?	Yes	☐	No	☐		
If yes to above, do you create them on information systems?	Yes	☐	No	☐		
Does your organization use National Security Systems?	Yes	☐	No	☐		

Requesting Official

Typed Name	Signature	Phone

Part 2 – Security Clearance Certification

The security clearances for the above named officials are correct.

Servicing Security Element Certifying Official

Typed Name	Signature	Date

Part 3 – AIN-1 Approval

To: (Requesting Line of Business or Office)

By FAA Order 1600.2, you have authority to set up a SCP or DCS and to appoint the officials identified in Part 1 to manage and operate your SCP or DCS.

Type Name	Signature	Date

Remarks:

FAA Form 1600.83

APPENDIX C. FOREIGN GOVERNMENT INFORMATION

This appendix describes additional measures for safeguarding foreign government information (FGI), other than North Atlantic Treaty Organization (NATO) information. United States Security Authority for NATO Instructions I-69 and I-70 address protective measures for NATO information. To the extent practical, and to promote its control, we store FGI separately from other classified information. To avoid extra costs, use methods such as using separate drawers of a container for separate storage. The safeguarding standards described below may be adjusted if required or permitted by treaties or agreements, or for other obligations, with the prior written consent of the National Security Authority of the originating government.

1. Top Secret.

a. Keep records of the receipt, internal distribution, destruction, access, reproduction, and transmittal;

b. Get consent of originating government before reproducing; and

c. Require witnessed destruction.

2. Secret.

a. Keep records of receipt, external dispatch and destruction;

b. Keep other records if required by the originator;

c. Reproduce only to meet mission needs unless prohibited by the originator; and

d. Keep reproduction records unless the originator waives this requirement.

3. Confidential. Keep records if the originator requires them.

4. Restricted and other foreign government information provided in confidence. To assure protection of other FGI provided in confidence (for example, foreign government "Restricted," "Designated," or unclassified provided in confidence), such information must be classified under EO 12958. We must provide a degree of protection to FGI at least equivalent to that required by the government or international organization that provided the information. When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that normally apply to US CONFIDENTIAL information. If the foreign protection requirement is lower than the protection required for US CONFIDENTIAL information, the following requirements apply:

a. Documents may retain their original foreign markings if the responsible agency determines that these markings are acceptable to meet the purposes served by U.S. classification markings. Otherwise, mark the documents: "This document contains (insert name of country)

(insert classification level) information to be treated as US (insert classification level)." The notation, "Modified Handling Authorized," may be added to either the foreign or U.S. markings authorized for foreign government information. If remarking foreign originated documents or matter is impractical, an approved cover sheet is an authorized option;

b. Disclose only to those who have a confirmed need-to-know, and where their official duties require access;

c. Notify individuals who have access of applicable handling instructions by a briefing, written instructions, or by applying specific handling requirements to an approved cover sheet;

d. Store in such a manner to prevent unauthorized access; and

e. Transmit in a method approved for classified information, unless the originating government waives this method.

5. Third-country transfers. The release or disclosure of foreign government information to any third-country entity must have the prior consent of the originating government if required by a treaty, agreement, bilateral exchange, or other obligation.

APPENDIX D. GUIDELINE FOR CISM SECURITY STANDARD OPERATING PROCEDURE (SOP)

The Classified Information Security Manager (CISM) must assess the vulnerability of classified information to unauthorized access. The CISM will use the assessment to develop a local security SOP instruction that follows this order and identifies local and unique handling procedures.

Include this information and procedures into the security instruction:

1. Purpose

2. Applicability

3. The basis for the local instruction, particularly this order

4. The security organization structure and identify security positions

5. Procedures for internal security reviews

6. Procedures for reporting and investigating unauthorized access, loss, compromise, or other security discrepancies

7. Procedures for security briefings and debriefings

8. Procedures for derivative classification to include identifying personnel in the organization who have derivative classification authority

9. Procedures for reviewing derivatively classified information to ensure correct classification and marking

10. If your organization has classified procurements, include industrial security procedures

11. Special controls on any types of classified information, for example, NATO classified

12. Procedures for reproducing classified information to include complying with limits and any special controls placed on information by originators

13. Procedures for safeguarding classified information to include:

- How to protect classified information during working hours
- How to store it when not in use
- How to screen incoming U.S. Postal Service Registered, Express, and Certified mail and shipments by cleared commercial carriers for classified information
- How to handcarry classified information

- How to protect it in a travel status
- Security container combination changes
- Location of records of security container combinations
- Emergency access to locked security containers
- Protecting telephone conversations
- Conducting classified meetings
- Automated Information Security processing procedures
- Reproduction equipment and controls
- Destruction equipment and procedures
- Visitor control procedures to allow visits involving access to, or disclosure of classified information – include procedures to verify personnel security clearances and need-to-know. Refer to Order 1600.1 for guidance on personnel security investigations, adjudications, and clearances.
- How to protect, remove, or destroy classified material in case of fire, natural disaster, civil disturbance, and other threats to minimize the risk of its compromise.

APPENDIX E. COURIER APPOINTMENT LETTER FORMAT

(Date)

SUBJECT: Authority to Hand-carry Classified Information

EXPIRATION DATE: (up to 1-year from date of letter)

ISSUING OFFICE: (Official mailing address)

TO: Whom it may concern

1. By FAA Order 1600.2, I approve the following individual to hand-carry classified information.

a. Name:

b. Grade:

c. Physical characteristics:

(1) Sex:

(2) Height:

(3) Hair Color:

(4) Eye Color:

d. Identification type and number:

2. Description of classified material: (Describe the material without revealing its classification or its contents.) For example:

One 8- by 11- inch sealed packaged addressed to the
Department of Energy, Office XYZ, Washington, DC, from
FAA Office Security and Hazardous Materials, ASH-X
800 Independence Ave, S.W.
Washington, DC. 20591

3. FAA point of contact for this letter: (Name and phone number, other than the courier, of official who can answer questions about the authorization).

(Signature and Title,
Manager, Servicing
Security Element, or
Activity/Office)

APPENDIX F. COURIER BRIEFING

The Federal Aviation Administration allows you to hand-carry classified information at the

☐ TOP SECRET ☐ SECRET level or below.

Your basic responsibilities while hand-carrying classified materials are to:

- Ensure you deliver it to the intended recipient;
- Protect it from disclosure to unauthorized people; and
- Report any problems in delivering the material to your manager and Classified Information Account Custodian (CIAC).

You must follow these procedures:

- Prepare an inventory of the material and leave copies of the inventory with your manager and CIAC;
- Ensure you double wrap or package the material:
  - ► You may use a briefcase as an outer wrapper only if you can lock it and your CIAC approves its use;
  - ► For air travel, you may not use a locked briefcase as an outer wrapper.
- Keep the material under your constant control always (You may not leave classified material unattended in vehicles, hotels, terminals or other unofficial public places);
- Arrange for overnight storage in a U.S. Government office or a cleared contractor facility, if you carry classified material on trips that involve an overnight stopover;
- Take reasonable precautions during unforeseen events – automobile accidents, theft, sudden illness – to prevent loss or compromise of the classified material;
- Do not reveal or discuss your courier duties with unauthorized people (You may reveal your duties to transportation screeners and you can allow your classified material to undergo screening by x-ray and explosive screening equipment);
- Do not discuss or display classified material in public places;
- Identify your intended recipient and get proper receipts for the classified material; and
- Do not use intoxicants while performing courier duties.

I certify that I have read this courier briefing, that I understand my courier duties, and that my questions, if any, have been satisfactorily answered.

Signature Date

APPENDIX G. RELATED PUBLICATIONS

The latest editions of these laws, regulations, orders, and standards make up the primary reference library for this order.

Public Law 107-347, the Federal Information Security Management Act (FISMA) of 2002. This law sets government-wide requirements for the security of information systems. It supercedes the Government Information Security Reform Act and the Computer Security Act. The FISMA provides the basis for identifying information systems as *national security systems*.

Executive Order (EO) 12829. This EO sets up the National Industrial Security Program to safeguard Federal Government classified information released to contractors, licensees, and grantees of the United States Government.

EO 12958, **as amended by EO 13292**. This EO prescribes the uniform system for classifying, safeguarding, and declassifying national security information

EO 12968. This EO sets up a uniform Federal personnel security program for employees who we consider for initial or continued access to classified information.

32 Code of Federal Regulations (CFR) Parts 2001 through 2004. These regulations give Federal agencies guidance on original and derivative classification, downgrading, declassification, and safeguarding of classified national security information.

49 CFR Part 8. These regulations set up procedures for classifying, declassifying, and disclosing classified information by elements of the DOT.

National Telecommunications and Information Systems Security Policy (NSTISSP) No. 6. This document contains national policy for certification and accreditation of National Security Systems

National Institute of Standards and Technology Special Publication 800-59, Guideline for Identifying an Information System as a National Security System. This document has guidelines for identifying an information system as a national security system.

National Security Agency Report #I333-015R-2005, Redacting with Confidence: How to Safely Publish Sanitized Reports Converted From Word to PDF. This report describes the issues of sanitizing Word and Adobe documents and gives step-by-step instructions on how to sanitize.

DOT Order 1640.4, Classified Information Management. This order contains the policies and assigns responsibilities for classifying, declassifying, and controlling classified information throughout the DOT.

Department of Defense Manual 5220.22-M, National Industrial Security Program Operating Manual. This manual prescribes requirements, restrictions, and other safeguards necessary to prevent unauthorized disclosure of classified information released by the U.S. Government Executive Branch Departments and Agencies to their contractors.

FAA Order 1000.36, FAA Writing Standards. This order sets up writing standards for all FAA Documents.

FAA Order 1270.1, Freedom of Information Act Program. This order administers the Freedom of Information Act (FOIA), 5 U.S.C. 552, at the FAA
FAA Order 1320.1, FAA Directives Management System. This order sets up the FAA system for issuing policy and procedures.

FAA Order 1350.14, Records Management. This order sets up the FAA Records Management Program.

FAA Order 1350.15, Records Organization, Transfer, and Destruction Standards. This order issues guidance to FAA employees for protecting and preserving valuable information.

FAA Order 1370.82, Information Systems Security Program. This order sets up policy and assigns responsibilities to implement the FAA's Information Systems Security Program.

FAA Order 1600.1, Personnel Security Program. This order sets up standards and procedures governing the FAA's Personnel Security Program.

FAA Order 1600.8, Communications Security (COMSEC) and Secure Voice. This order sets up FAA policy and procedures and assigns responsibilities to comply with national COMSEC policy.

FAA Order 1600.12, Technical Surveillance Countermeasures Program (TSCM). This order sets up the FAA's TSCM Program.

FAA Order 1600.69, FAA Facility Security Management Program. This order sets up security requirements to protect FAA facilities and people.

FAA Order 1600.72, Contractor and Industrial Security Program. This order sets up policies and responsibilities for implementing the FAA's Industrial Security Program.

FAA Order 1600.74, Visitor Procedures for Federal Aviation Administration Facilities. This order sets up policy for allowing visitors access to FAA facilities and information.

FAA Order 1600.75, Protecting Sensitive Unclassified Information. This order sets FAA policy and guidance for protecting sensitive unclassified information (SUI).

FAA Order 1900.1, FAA Emergency Operations Plan. This order sets up the FAA's emergency operations plan.

Information Security Oversight Office (ISOO) Marking Booklet. The booklet provides guidelines on marking classified information. It is available at http://www.archives/gov/isoo/ under the Education, Training, and Materials link.

National Security Agency Report # I333-015R-2005, Redacting with Confidence: How to Safely Publish Sanitized Reports Converted From Word to PDF. This paper describes the pitfalls of sanitizing – redacting – a Word document and gives step-by-step instructions on how to do it with confidence so that you do not disclose classified information.

APPENDIX H. USING SECURE TELEPHONES

Your telephone calls are at risk of interception at any point during your telephone conversation. The Government developed a special class of telephones to encrypt the conversations over the telephone lines to prevent eavesdropping. This appendix discusses this special class of telephones and their use. For more information on security telecommunications equipment and its uses, see FAA Order 1600.8.

RESPONSIBILITIES AND REQUIREMENTS:

You must not discuss classified information over unsecured telephone lines. Anyone wishing to discuss classified national defense information over the telephone must ensure they use secure telephone equipment. The STU-III (Secure Telephone Unit–third generation) and STE (Secure Terminal Equipment) are special telephone instruments that callers can switch to a secure mode for discussion of classified information.

If you need to discuss classified information, you can use the secure telephone in nonsecure mode to place a call to another party who also has a secure telephone. After a caller makes a connection, the caller asks the party receiving the call to "go secure." You and the other party then put your crypto-ignition keys (CIKs) or Fortezza cards, described below, into the phone terminal, turn them on and press the SECURE button. It may take about 15 seconds to set up a secure connection. If you have a secure connection, the display screen on the unit shows the highest classification level at which discussion is authorized. After hanging up, wait at least two seconds before removing the CIK/card.

What is the greatest risk associated with the secure telephone? It is the supposedly unclassified chitchat that goes on before the secure telephone is in a secure mode. A defector from an intelligence service that intercepts U.S. communications reports that encrypted secure telephone conversations are unbreakable, but the discussions before activating and after deactivating secure encryption, are a bonanza of valuable information. It is not difficult for communications intercepts to identify the phone numbers linked to secure telephones. Since we use the same numbers for encrypted and unencrypted conversations, these numbers are high priority targets.

The secure telephone instrument itself is not classified. We can install and use these instruments in any room where we allow classified conversations.

Special rules apply to protecting the CIK or Fortezza card that turns the secure telephone from a regular telephone into a secure telephone.

- The CIK, KSD-64A, activates the secure mode of the STU-III. It looks similar to a car key, but it contains an electronically erasable programmable read-only memory chip (EEPROM). The CIK stores an electronic password which allows you to use the secure features of a particular secure telephone. We can program a CIK to store other information. The rules for protecting it vary depending on what information we store on it.

- The Fortezza card is about the size of a thick credit card and performs essentially the same way as the CIK, but with more capabilities.
- When we program the CIK or Fortezza card to encrypt our telephone conversations, you must protect it as follows:

FIGURE H-1 – Protecting the CIK or Fortezza Card	
If CIK or Fortezza card	*Then*
Are in the same room as the secure telephone	◆ The CIK or Fortezza card must be under the personal control of an authorized person; or ◆ Store them in a GSA approved security container
Are not in the same room as the secure telephone equipment	◆ Protect them as high-value property; ◆ You may store them in a locked cabinet or desk; or ◆ An authorized person may keep it in their personal possession.

Unauthorized use or loss of CIKs or Fortezza Cards. You must report unauthorized use or loss of the KSD-64A or Fortezza Card to your regional Servicing Security Element.

RECORD OF CHANGES

DIRECTIVE NO. **1600.2E**

CHANGE TO BASIC	SUPPLEMENTS			OPTIONAL	CHANGE TO BASIC	SUPPLEMENTS			OPTIONAL