



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

ORDER
1600.75

Effective Date:
Feb. 1, 2005

SUBJ: PROTECTING SENSITIVE UNCLASSIFIED INFORMATION (SUI)

In the aftermath of September 11, 2001, there is heightened awareness of the need to safeguard sensitive Government information that does not meet the standards for classified national security information. Of particular concern is our need to protect Government information related to homeland security. This includes information that supports the FAA global aerospace structure that contributes to the security of the nation and public safety. This order provides agency policy and guidance for protecting sensitive unclassified information we create or control.

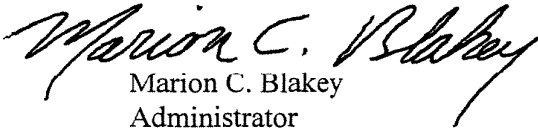

Marion C. Blakey
Administrator
Federal Aviation Administration

TABLE OF CONTENTS

CHAPTER 1. GENERAL INFORMATION

1. What is the purpose of this order?	1-1
2. Who does this order affect?	1-1
3. What documents does this order cancel?	1-1
4. What is sensitive unclassified information?	1-1
5. How do I decide which designation is appropriate?	1-2
6. Are there other types of sensitive unclassified information?	1-3
7. I'm not sure if my unclassified information is sensitive or not, what should I do?	1-4
8. What is the difference between classified information and sensitive unclassified information?	1-4
9. How do the Freedom of Information Act and Privacy Act relate to sensitive unclassified information?	1-4
10. How does the Federal Service Labor-Management Relations Statute relate to sensitive unclassified information?	1-5
11. What responsibilities do FAA offices and individuals have for this order?	1-5
12. What Federal laws, regulations, and guidance primarily apply to this order?	1-7
13. What DOT and FAA orders and policies primarily apply to this order?	1-7

CHAPTER 2. ACCESS AND DISCLOSURE

1. When may persons have access to sensitive unclassified information?	2-1
2. What is duty to protect?	2-1
3. What is need-to-know?	2-2
4. If sensitive unclassified information is unprotected or disclosed to unauthorized persons, what should I do?	2-4
5. Can I be disciplined if I make an unauthorized disclosure?	2-4

CHAPTER 3. SENSITIVE UNCLASSIFIED INFORMATION PROTECTIVE MEASURES

1. What is the purpose of protective measures?	3-1
2. Does a manager have flexibility in selecting and implementing protective measures?	3-1
3. Why do I mark?	3-1
4. Is sensitive unclassified information always marked?	3-1
5. When do I mark?	3-2
6. How do I mark?	3-2
7. How do I protect sensitive unclassified information during working hours?	3-3
8. How do I protect sensitive unclassified information after working hours?	3-3
9. May I make copies of sensitive unclassified information?	3-3
10. May I work on sensitive unclassified information at home or while on travel?	3-3
11. How must I handle sensitive unclassified information if I telecommute?	3-4
12. How do I hand carry, mail, or ship sensitive unclassified information?	3-4
13. May I discuss sensitive unclassified information over the telephone?	3-4
14. May I fax sensitive unclassified information?	3-4
15. How do I protect sensitive unclassified electronic mail?	3-5
16. May I post sensitive unclassified information to web sites?	3-5

17. How do I destroy paper documents and records?	3-5
18. How do I destroy electronic records?	3-6
19. What should I do when sensitive unclassified information no longer needs protection?	3-6

CHAPTER 4. ADMINISTRATIVE INFORMATION

1. Distribution of this Order	4-1
2. Who has authority to change or supplement this order?	4-1
3. Who do I contact if I have a question about this order	4-1
4. Where can I get more information about this order?	4-1

APPENDICES

APPENDIX A

Information Comprising Sensitive Security Information

APPENDIX B

Federal laws, regulations, and guidance

APPENDIX C

DOT and FAA orders and policies

APPENDIX D

Marking For Official Use Only Information

APPENDIX E

Marking Sensitive Security Information

APPENDIX F

Summary of Protective Measures

CHAPTER 1. GENERAL INFORMATION

1. What is the purpose of this order?

a. This order provides guidance for identifying and protecting sensitive unclassified information (SUI). Specifically, the order:

- (1) Defines the term “sensitive unclassified information” for the FAA;
- (2) Assigns responsibilities to FAA offices and individuals for SUI;
- (3) Discusses the conditions for SUI access and disclosure; and
- (4) Issues basic policy, procedures, and guidance for protecting SUI.

b. This order *does not* modify, amend, cancel, supplant or replace FAA orders about implementing and administering the Freedom of Information Act or Privacy Act, officials responsible for these programs, or lines of business responsibilities under the programs.

2. **Who does this order affect?** This order applies to every FAA employee, contractor, consultant, and grantee who creates, handles, or has access to SUI.

3. **What documents does this order cancel?** This order cancels:

a. 9-AWA-Broadcast message of July 16, 2004, Subject: Interim Guidelines – Sensitive Security Information;

b. Appendix 10 to FAA Order 1600.2D, Requirements for Protecting Sensitive But Unclassified Information; and

c. ASH (formerly ACS) Policy Memorandum Number ACP-300-01-001, Safeguarding and Control of Sensitive Security Information.

4. **What is Sensitive Unclassified Information (SUI)?** SUI is unclassified information – *in any form including print, electronic, visual, or aural forms* - that we must protect from uncontrolled release to persons outside the FAA and indiscriminate dissemination within the FAA. It includes aviation security, homeland security, and protected critical infrastructure information. SUI may include information that may qualify for withholding from the public under the Freedom of Information Act (FOIA). Throughout the Federal government there are over 50 types of SUI, but within the FAA we generally handle four types:

a. **For Official Use Only (FOUO) information.** FOUO is the *primary* designation given to SUI by the Department of Transportation (DOT) and FAA. It consists of information that could adversely affect the national interest, the conduct of Federal programs, or the privacy of individuals if released to unauthorized individuals. As examples, the uncontrolled use of FOUO information may allow someone to:

- or
- (1) Circumvent agency laws, regulations, legal standards, or security protective measures
 - (2) Obtain unauthorized access to an information system.

b. Sensitive Security Information (SSI). SSI is a designation *unique* to the DOT and DOT's operating administrations and to the Department of Homeland Security (DHS). It applies to information we obtain or develop while conducting *security activities*, including research and development activities. Unauthorized disclosure of SSI would:

- (1) Constitute an unwarranted invasion of privacy (including, but not limited to, information contained in any personnel, medical, or similar file);
- (2) Reveal trade secrets or privileged or confidential information obtained from any person; or
- (3) Be detrimental to transportation safety or security.

c. Sensitive Homeland Security Information (SHSI). SHSI is a designation *unique* to homeland security information that we share with State and local personnel. The Federal government shares SHSI with State and local personnel who are involved in prevention against, preparation for, or response to terrorism. We protect it because its loss, misuse, unauthorized disclosure or access, or modification can significantly impair the capabilities and efforts of Federal, State, and local personnel to predict, analyze, investigate, deter, prevent, protect against, mitigate the effects of, or recover from acts of terrorism. If our sensitive unclassified information impairs these capabilities, we must designate it SHSI before we share it with State and local personnel to facilitate its proper protection. See also Chapter 2, paragraphs 2.c and 3.c.

d. Protected Critical Infrastructure Information (PCII). PCII is a designation *unique* to critical infrastructure information provided by non-government persons and entities to the DHS. DHS uses the information for security of critical infrastructure and protected systems, analysis, warning, interdependency studies, recovery, reconstitution, or other informational purposes. While only DHS can designate information as PCII, they can share it with other Federal agencies as needed for operational purposes. PCII is defined in 6 CFR Part 29.1. See also Chapter 2, paragraphs 2.d and 3.d.

5. How do I decide which designation is appropriate? At times For Official Use Only, Sensitive Security Information, Sensitive Homeland Security Information, and Protected Critical Infrastructure Information designations appear to overlap. However, each designation supports common aims, which are to protect the information from uncontrolled release outside the FAA and indiscriminate dissemination within the FAA. The primary factors for determining the appropriate designation are the information's subject matter and intended audience.

a. For Official Use Only information

- (1) Subject matter. Information, *including non-security information*, that may qualify for withholding from the public under FOIA exemptions 2 through 9. (FAA Order 1270.1)

(2) Intended audience. Federal employees, contractors, and grantees.

b. Sensitive Security Information

(1) Subject matter. *Security information* listed in 49 CFR Part 15.5 and Appendix A.

(2) Intended audience. *Covered Persons* specified by 49 CFR Part 15.7 and Chapter 2, paragraph 2.b.

(3) Other factors: FOIA exemption 3 applies.

c. Sensitive Homeland Security Information (SHSI)

(1) Subject matter. Information dealing with predicting, analyzing, investigating, deterring, preventing, protecting against, mitigating the effects of, or recovering from acts of terrorism.

(2) Intended audience. State and local personnel as defined by the Homeland Security Act of 2002.

(3) Other factors:

- SHSI must be tailored information products appropriate for sharing with State and local personnel
- FOIA exemption 3 applies

d. Protected Critical Infrastructure Information (PCII)

(1) Subject matter. Non-Federal information, voluntarily submitted by the private sector pertaining to critical infrastructure as defined by 6 CFR Part 29.2.

(2) Intended audience. Federal agencies, U.S. government authorities, U.S. Government contractors, and foreign, State, and local government authorities

(3) Other factors:

- Only the Department of Homeland Security (DHS) can designate information PCII;
- DHS must approve all disclosures
- FOIA exemption 3 applies

6. Are there other types of sensitive unclassified information (SUI)? Yes,

a. Variable terminology and markings. Other Federal agencies use different terminology and markings to designate SUI. For example, the Department of Energy uses Official Use Only

(OUO), the Department of State uses Sensitive But Unclassified (SBU), and the Drug Enforcement Administration uses DEA Sensitive. Many Federal law enforcement agencies use the term Law Enforcement Sensitive (LES).

b. Foreign government information. Additionally, foreign governments may share their restricted information or information provided in confidence with us under treaty, agreement, bilateral exchange, or other obligation.

c. Sensitive non-government information. Contractors, grantees, businesses, regulated parties, and other non-government entities share sensitive information with us that they mark as business sensitive, confidential, proprietary, trade secret, and so on. You must also protect this information from unauthorized disclosure. Unless greater protective measures are specified by the information's originator, protect it as FOUO information.

d. Overlapping and inconsistent policies. Since there are over 50 different types of SUI used amongst U.S. Government agencies, there will be policy and procedural variation that may not be consistent with this order. Refer questions regarding overlapping and inconsistent policies to your Servicing Security Element (SSE). In regions your SSE is the Security and Hazardous Materials Division, AXX-700; at the Washington Headquarters, the SSE is the Office of Internal Security, AIN-1.

7. I'm not sure if my information is sensitive unclassified information or not, what should I do?

a. Protect it. If you're not sure protect it as FOUO information.

b. Contact your Security Servicing Element. Your SSE can answer any questions regarding SUI designators and protective measures.

8. What is the difference between classified information and sensitive unclassified information? Both types are sensitive and both types have restrictions on access and disclosure. The differences are found in the degree of sensitivity, the rules for access and protection, and the damage that results from unauthorized disclosure. FAA Order 1600.2 provides directions for protecting classified information.

9. How do the Freedom of Information Act (FOIA) and Privacy Act relate to sensitive unclassified information? The FOIA and Privacy Act impose statutorily defined rights and obligations that agencies must observe, regardless of whether or not we designate the information as SUI.

a. Freedom of Information Act requests. If we receive a FOIA request for SUI, we must evaluate the information at that time and determine in each case whether a FOIA exemption applies. See FAA Order 1270.1 for details of the FAA's FOIA program and for explanations of FOIA exemptions.

b. Privacy Act. Similarly, the Privacy Act restricts how we collect, maintain, and disseminate personal information and make it available to the person. (FAA Order 1280.1)

10. How does the Federal Service Labor-Management Relations Statute relate to sensitive unclassified information? If we receive a request for SUI under Section 7114(b)(4) of the Federal Service Labor-Management Relations Statute, we must evaluate the information at that time and determine in each case whether Section 7114(b) (4) applies.

11. What responsibilities do FAA offices and individuals have for this order?

a. The Assistant Administrator for Security and Hazardous Materials, ASH-1. ASH-1 provides agency-wide policy and procedures for protecting classified national security information and sensitive unclassified information. ASH-1 is also the FAA's Senior Agency Official for protecting classified information under Executive Order (E.O.) 12958, as amended, Classified National Security Information. FAA Order 1600.2 implements the E.O. within the FAA and addresses policies and procedures for classified information. ASH-1, through the Office of Internal Security, AIN-1:

(1) Evaluates the effectiveness of FAA information security policies, procedures, and practices for protecting classified and SUI;

(2) Provides advice and assistance to FAA managers on protecting classified information and SUI;

(3) Establishes a SUI security education and awareness program;

(4) Appoints a Protected Critical Infrastructure Information (PCII) Officer, who performs the responsibilities specified by 6 CFR Part 29 and manages the FAA's PCII program; and

(5) Appoints a Sensitive Homeland Security information (SHSI) Program Officer, who manages the FAA's SHSI program as directed by the Department of Homeland Security SHSI Program Officer.

b. The Assistant Administrator for Information Services, AIO-1. AIO-1 provides agency-wide oversight for protecting FAA information systems and the information they contain. This includes protecting SUI while within these systems. (FAA Orders 1370.81 and 1370.82)

c. FAA Managers :

(1) Identify and protect SUI that supports their operations and assets. Protection efforts must focus on preventing unauthorized or inadvertent disclosure, particularly when visitors enter areas where we use or process SUI. FAA Order 1600.74 addresses our policies and procedures for allowing visitors access to our facilities and information.

(2) Stay aware of both the surreptitious and accidental threats posed by personal computer and communication devices carried by employees and visitors. Where these devices

pose a threat, managers should implement protective measures to mitigate the threat. Depending on the device and technology, appropriate protective measures may range from controlling to banning their use in areas where SUI is discussed or processed. Such devices include:

- Cell phones (with picture-taking capabilities),
- Personal Data Assistants (PDAs),
- Pocket PC's,
- Multi-functional pagers,
- Any device for taking video/photographic images,
- Flash drives, and
- Any other devices capable of storing, processing, or transmitting information

(3) Make their employees aware of the policies and procedures of this order.

(4) Require appropriate security clauses for personnel, facilities, and information protection through the acquisition process of contracts or grants that require access to SUI.

(5) Ensure their websites, if available to the public, do not contain or provide links to SUI.

(6) Assess the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of the SUI that support their operations and assets.

(7) While planning for emergencies and Continuity of Operations (COOP), identify and protect SUI necessary to perform essential functions and to reconstitute normal operations after the emergency.

(8) If there is an unauthorized disclosure, take appropriate actions to:

- *Mitigate the consequences* of the disclosure;
- *Correct the conditions* that caused the disclosure;
- *Assess the harm* of the disclosure; and
- *Notify the originator* of the information, and in the case of Sensitive Security Information, SHSI, or PCII notify their supporting SSE or AIN-1.

(9) Periodically audit protective measures to determine if the measures are meeting their needs.

(10) Refer questions, concerns, and issues to their supporting Servicing Security Element.

d. FAA Employees. Employees should familiarize themselves with the requirements in this order. When an employee has custody or control of SUI, their *basic obligation* is to ensure that unauthorized persons do not gain access to it.

12. What Federal laws, regulations, and guidance primarily apply to this order?
See Appendix B.

13. What DOT and FAA orders and policies primarily apply to this order? See Appendix C.

CHAPTER 2 – ACCESS AND DISCLOSURE

1. When may persons have access to sensitive unclassified information (SUI)? In general, persons must have a *duty to protect* the information and then a *need-to-know* it before they may have access to SUI. The holder of the information determines if these qualifications are met as described in the following paragraphs.

2. What is duty to protect? This means the recipient of the information has a duty imposed by law, regulation, or contractual agreement to protect the information from unauthorized access and disclosure. The precise meaning of the term varies depending on the type of sensitive unclassified information.

a. For Official Use Only (FOUO) and other agency SUI:

(1) Agency standards of conduct address a government employee's duty to protect FOUO and other agency SUI. (FAA Human Resources Policy Manual, ER 4-1, Standards of Conduct)

(2) A DOT or FAA contractor, consultant, grantee, or licensee has a duty to protect FOUO and other agency SUI when appropriate personnel suitability investigations have been completed (FAA Order 1600.73), and their contract or agreement contains clauses legally binding them to protect the information from unauthorized disclosure. Clauses must include information on safeguarding standards, and the contractor, consultant, or grantee must complete a non-disclosure agreement. For details on writing security clauses, go to the Contract Writing Toolbox in the FAA Acquisition System Toolset at <http://fast.faa.gov>.

b. Sensitive Security Information (SSI). 49 CFR Part 15.7 uses the term *covered persons* to identify those who have a duty to protect SSI. *Covered persons* include:

(1) Each airport operator and aircraft operator subject to the requirements of Subchapter C of 49 CFR;

(2) Each indirect air carrier, as defined in 49 CFR Part 1540.5;

(3) Each owner, charterer, or operator of a vessel, including foreign vessel owners, charterers, and operators, required to have a security plan under Federal or international law;

(4) Each owner or operator of a maritime facility required to have a security plan under the Maritime Transportation Security Act;

(5) Each person performing the function of a computer reservation system or global distribution system for airline passenger information;

(6) Each person participating in a national or area security committee established under 46 U.S.C. 70112, or a port security committee;

(7) Each industry trade association that represents covered persons and has entered into a non-disclosure agreement with any organizational element of the Department of Homeland Security (DHS) or DOT;

(8) Any organizational element of the DHS and DOT and their employees;

(9) Each person conducting research and development activities that relate to aviation and or maritime transportation security and are approved, accepted, funded, recommended , or directed by any organizational element of the DHS or DOT;

(10) Each person who has access to SSI as specified in 49 CFR Part 15.11;

(11) Each person employed by, contracted to, or acting for a covered person, including a grantee of any organizational element of the DHS or DOT, and including a person formerly in such positions;

(12) Each person for which a vulnerability assessment has been directed, created, held, funded, or approved by any organizational element of the DOT and DHS, or that has prepared a vulnerability assessment that will be provided to any organizational element of the DOT or DHS in support of a Federal security program; and

(13) Each person receiving SSI under 49 CFR Parts enforcement proceedings or under conditional disclosure procedures.

c. Sensitive Homeland Security Information. Section 892 of the Homeland Security Act of 2002 authorizes sharing of homeland security information with:

(1) Federal agencies and their employees; and

(2) State and local entities and persons.

d. Protected Critical Infrastructure Information (PCII). 6 CFR Part 29.8 authorizes disclosure of PCII to support lawful and authorized Government purposes to:

(1) Federal government employees;

(2) State and local government entities who have a written agreement with the DHS PCII Program Manager; and

(3) Federal contractors who have signed corporate and or individual confidentiality agreements with the DHS PCII Program Manager or our PCII Officer.

3. What is need-to-know? Need-to-know is a fundamental security principle that limits the flow of information only to those who need it to perform authorized government functions or services. Need-to-know may be generally determined as follows:

a. For Official Use Only information: Subject to the limits of the Privacy Act, you may disclose FOUO information to a person who has a duty to protect it (see paragraph 2.a.(1) above) when the person needs the information to perform or assist in any lawful and authorized government function.

b. Sensitive Security Information: You may disclose SSI to a person who has a duty to protect it when:

(1) The person needs *specific SSI* to carry out transportation security activities approved, accepted, funded, recommended, or directed by any organizational element of the DOT or DHS;

(2) The person is in training to carry out transportation security activities approved, accepted, funded, recommended, or directed by DOT and its operating administrations, or DHS;

(3) The information is necessary for the person to supervise or otherwise manage individuals carrying out transportation security activities approved, accepted, funded, recommended, or directed by DOT and its operating administrations, or DHS;

(4) The person needs the information to provide technical or legal advice to a covered person regarding transportation security requirements of Federal law;

(5) The person needs the information to represent a covered person in connection with any judicial or administrative proceedings regarding those requirements;

(6) Federal employees, if access is necessary for performance of the employee's official duties; and

(7) Federal contractors and grantees, if access is necessary to performance of the contract or grant.

c. Sensitive Homeland Security Information. When State and local personnel need the information to perform, assist in, prepare for, be forewarned of, respond to, and participate in plans, operations, actions or events related to homeland security.

d. Protected Critical Infrastructure Information. You may disclose PCII to other FAA employees to support lawful and authorized Government purposes. The PCII Officer must approve all other disclosures.

e. Other-agency sensitive unclassified information. If the agency does not put disclosure restrictions on their SUI in a warning or disclosure statement, you may disclose their SUI to a person who has a duty to protect it and when the person needs the information to perform or assist in any lawful and authorized government function. If you're unsure about disclosing other-agency information, you should consult with the originating agency before you disclose it.

f. Foreign government information. You determine need-to-know by the treaty, agreement, bilateral exchange, or other obligation by which the foreign government provided the

information to the FAA.

4. If sensitive unclassified information is unprotected or disclosed to unauthorized persons, what should I do?

- a. Protect.** Protect the information if possible ; and
- b. Report.** Report the incident to your management chain of command as soon as possible.

5. Can I be disciplined if I make an unauthorized disclosure? Yes. Each line of business and staff office is responsible for determining whether to pursue any conduct or disciplinary action against employees under their authority.

- a. Employee standards of conduct.** FAA standards of conduct address discipline for employees who disclose information not authorized by law or agency policy.
- b. Sensitive Security Information.** Employees who violate SSI provisions of 49 CFR Parts 15 and 1520 may also be subject to appropriate civil penalty.
- c. Protected Critical Infrastructure Information.** Federal employees may be subject to criminal penalties: fines and imprisonment of not more than one year, or both, and must be removed from office or employment.

CHAPTER 3. SENSITIVE UNCLASSIFIED INFORMATION PROTECTIVE MEASURES

1. What is the purpose of protective measures? We use protective measures to safeguard sensitive unclassified information (SUI) from uncontrolled release outside the FAA and indiscriminate dissemination within the FAA. Protective measures start with marking and end when we cancel markings or destroy records.

2. Does a manager have flexibility in selecting and implementing protective measures? Yes.

a. Minimum level of protection. This order addresses a minimum level of protection for SUI. Managers may implement *additional* measures when their SUI needs a higher level of protection. Regional and Center Servicing Security Elements (SSE) can help managers tailor protective measures to meet a particular need.

b. Information System Security Plan (ISSP). The ISSP identifies information system components; operational environment; sensitivity and risks; and detailed, cost-effective measures to protect a system and the information it contains. Commensurate with the risk and magnitude of harm from unauthorized disclosure, the ISSP spells out measures to protect SUI within the system. ISSP protective measures might exceed those of this order. (FAA Order 1370.82 and FAA Information Security Program Handbook, latest version)

3. Why do I mark?

a. Basic protective measure. Marking is a basic protective measure that draws a reader's attention to the sensitivity of information and the need to protect it.

b. Disclosure aid. Marking helps us make disclosure decisions and to select and apply appropriate protective measures.

c. Marking is not conclusive proof of sensitivity. When we receive a Freedom of Information Act (FOIA) request for SUI, we must evaluate the information to determine whether a FOIA exemption applies to the request. Then we must follow FOIA procedures to determine whether to withhold the information or any portions of it from the public. Information sensitivity may cease because of the passage of time or change in circumstances.

4. Is sensitive unclassified information always marked? No.

a. Errors and changing sensitivities. Because of error or changing sensitivities, you may come across

(1) Unmarked SUI that should be marked or

(2) Information that is marked but is no longer sensitive.

b. Freedom of Information Act (FOIA) requests. When we receive a request for any official document under the FOIA, we should evaluate it from an SUI perspective whether or not it is marked.

c. Questioned markings. If you're unsure about markings, contact your supporting SSE for a resolution and protect the questioned information as though it were For Official Use Only (FOUO) information pending resolution of your case.

5. When do I mark? Mark information when you create it or determine that it meets the standards of sensitive unclassified information. Exceptions:

a. Records in storage. If you have unmarked records in storage that should be marked, you do not need to remove them from storage only to mark them. Mark them when you remove them from storage for other purposes.

b. Records marked under old authority. You may come across information marked under an old regulatory authority, e.g., 14 CFR § 191 for Sensitive Security Information, and find it marked differently than directed by this order. You do not need to remark these documents.

c. Sensitive non-government information. Your office may receive information from contractors, grantees, businesses, and regulated parties marked as business sensitive, confidential, proprietary, trade secret, and so on. You do not need to remark this information, but you must protect it from unauthorized disclosure. Unless greater protective measures are specified by the information's originator, protect it as FOUO information.

6. How do I mark?

a. Marking guides. See Appendices D and E for marking FOUO information and SSI, which have different marking protocols. Our Sensitive Homeland Security Information (SHSI) Program Officer and Protected Critical Infrastructure Information (PCII) Officer will issue separate marking guidance for SHSI and PCII.

b. Sensitive unclassified information markings in classified records. When marking documents and other material containing both classified national security information and SUI, refer to FAA Order 1600.2.

c. Marking other sensitive unclassified records. Mark other records, such as photographs, films, tapes, slides, or records residing in information systems with appropriate protective markings and distribution limitation statements in a conspicuous way so that persons having access to them are aware of their sensitivity.

d. Marking removable electronic storage media. Mark removable electronic media, e.g., diskettes and compact disks, with the appropriate protective marking and distribution limitation statement in a conspicuous way so that persons having access to them are aware of their sensitivity. The ISSP for a system will contain specific measures for labeling and marking removable media.

e. Sharing sensitive unclassified information with agencies outside the DOT. When you send SUI records outside the DOT, you should include supplementary markings and notices to explain the significance of the information and to promote its proper handling. For example, you should include a statement such as the following in a transmittal record or directly on the record containing SUI.

This document/record belongs to the Federal Aviation Administration and may be used for official government purposes only. It may not be released without the express permission of the Federal Aviation Administration. Refer requests for the document to: (insert name and address of originating office.)

7. How do I protect sensitive unclassified information during working hours? During working hours, you must take reasonable steps to minimize the risk of access by unauthorized persons. Such steps include

a. Physical custody or control. When SUI is not in secure storage, it must be under the protection and control of an authorized person.

b. Cover sheets. You may use DOT Form 1600.7-1, For Official Use Only Cover Sheet, or other appropriate cover sheet to prevent inadvertent or casual disclosure to unauthorized persons.

c. Not under physical custody or control. When your SUI is not under the physical custody or control of an authorized person, you must store it in a lockable container, such as a file cabinet or desk, or in a locked space. Your office must control the keys to the locks of these containers and spaces, and key holders must be authorized persons.

8. How do I protect sensitive unclassified information after working hours?

a. Uncontrolled work spaces. If your work area is accessible to persons, who are not authorized access to your SUI, you must store your SUI in a secure container such as a locked desk, file cabinet, or an inaccessible locked space. Your office must control the keys to the locks of these containers and spaces, and key holders must be authorized persons.

b. Controlled work spaces. If your work area is accessible only to persons who are authorized access to your SUI, you do not need additional protective measures. Again your office must control the keys to the locks for controlled work spaces.

9. May I make copies of sensitive unclassified information? You may reproduce SUI on regular office copiers to the extent needed to carry out official business. Other precautions:

a. Mark and protect. Mark and protect copies in the same manner as the original.

b. Destroy unused copies and copying residue. Properly destroy unused copies and copying residue. See paragraph 17.

10. May I work on sensitive unclassified information at home or while on travel? Yes, but

working on SUI outside your workplace poses additional security risks and challenges. If you need to work with SUI at home or while on travel, you must have your manager's approval to do so. Remember that, as the holder of SUI, you are responsible for protecting it from unauthorized disclosure while you are at home or traveling.

11. How must I handle sensitive unclassified information if I telecommute? Under the FAA Telecommuting Handbook of 1997, whether telecommuting from home or at a telecommuting center, you must provide the same level of protection for the information that you do from your normal work site. Your manager must approve specific protective measures for handling paper records, and your information systems security manager must certify the adequacy of security for off-site access to sensitive data. See paragraph 15 for protecting sensitive email.

12. How do I hand carry, mail, or ship sensitive unclassified information? You may hand carry, mail, or ship it in any manner that prevents inadvertent disclosure of the contents.

a. Hand carrying. Place the information in an opaque envelope or carry it within a brief case, pad folio, or other container. For FOUO information, you may use DOT Form 1600.7-1, FOUO Cover Sheet, or the FAA Form 1360-39, FOUO Envelope, if available.

b. Interoffice mail. Use a sealed opaque envelope with the addressee indicated on it. This is in addition to or instead of any office messenger envelopes. If available, you may use the FAA Form 1360-39.

c. U.S. or Contract Mail. Mail or send documents and materials in properly addressed opaque envelopes or containers by United States Postal Service first-class, certified, or registered mail or contracted delivery service. You may send bulk shipments, such as directives, by fourth-class mail when you wrap the shipment in opaque covering.

13. May I discuss sensitive unclassified information over the telephone? Yes, but confirm that you are speaking to an authorized person before discussing the information, and inform the person that your discussion will include SUI and what part of the discussion is sensitive. Never leave voicemail messages containing SUI.

14. May I fax sensitive unclassified information? Yes, but:

a. Mark your fax. Ensure that you appropriately mark the documents you are faxing;

b. Send to correct number. Use special care to ensure that you are sending your documents to the correct fax number; and

c. Determine how faxes are handled at the receiving end:

(1) If you are sending the fax to a controlled area, where only authorized persons will have access to it, then you may send it without further precautions.

(2) If you are sending the fax to an uncontrolled area, where unauthorized persons might

have access to it, then request that an authorized person stand by at the receiving end as you send the fax. Ask them to confirm receipt.

15. How do I protect sensitive unclassified electronic mail?

a. Mark. You must mark emails in the subject line “For Official Use Only” or “Sensitive Security Information” as appropriate. If you’re sending sensitive unclassified attachments, ensure you appropriately mark them following Appendices D and E.

b. Encrypt. You must also follow the security and encryption procedures of FAA Order 1370.81.

16. May I post sensitive unclassified information to web sites?

a. Unsecure Internet web sites. You may not post SUI to an unsecured web site that can be accessed by the public from the Internet. Public web sites must not provide links to web sites where we post SUI. (FAA Order 1370.79)

b. Secure Intranet web sites. You may post SUI to restricted FAA web sites provided they have special logon protocols and password protection. You may give passwords to these sites only to persons who satisfy the “duty to protect” and “need-to-know” requirements explained in chapter 2.

17. How do I destroy paper documents and records?

Destruction Standards for Paper Documents and Records		
If your document is	Then your destruction standard is	Method
FOUO	To make recognition and reconstruction difficult	At a minimum, tearing or shredding each page into small pieces and mixing those pieces into regular trash
SSI	completely to preclude recognition or reconstruction	burning, shredding, wet-pulping and chemical decomposition (Note 1)
SHSI	By any means approved for destruction of classified information or by any other means that would make it difficult to recognize or reconstruct the information	burning, cross-cut shredding, wet-pulping and chemical decomposition
PCII	By any method that prevents unauthorized retrieval	burning, cross-cut shredding, wet-pulping and chemical decomposition
Note 1: You may use existing strip shredders, but any new shredding equipment must have a cross-cut feature. Your supporting SSE can provide assistance in selecting an appropriate destruction method and equipment.		

18. How do I destroy electronic records? The Security Certification and Accreditation Package for each information system should include specific procedures for administratively canceling sensitive unclassified markings in storage media; clearing or sanitizing sensitive information from storage media; or destroying media storing sensitive information. (FAA Order 1370.82)

19. What should I do when sensitive unclassified information no longer needs protection?

a. If you're the originator of For Official Use Only or Sensitive Security Information. You may cancel a record's sensitive unclassified status when circumstances indicate that the record no longer needs protection. If practical, you should notify all known holders that the record is no longer sensitive.

b. If someone else is the originator of For Official Use Only or Sensitive Security Information. If you believe the information no longer requires protection, you should notify the originator giving a reason or reasons why restrictions on access and disclosure are no longer necessary. If you cannot identify the information's originator, refer the matter to AIN-1 through your supporting Servicing Security Element.

c. If the information is Sensitive Homeland Security Information or Protected Critical Infrastructure Information. You must coordinate with our SHSI Program Officer or our PCII Officer.

CHAPTER 4. ADMINISTRATIVE INFORMATION

1. **Distribution of this order.** Distribute order to

- a. Branch level and above at the Washington and regional headquarters;
- b. Branch level and above at the Mike Monroney Aeronautical Center and the FAA Technical Center;
- c. All field facilities; and
- d. All FAA contract towers.
- e. This order is also electronically available at <http://dmis.faa.gov>.

2. **Who has authority to change or supplement this order?**

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

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

3. **Who do I contact if I have a question about this order?** Your Servicing Security Element (SSE) will answer any questions regarding the order. In regions your SSE is the Security and Hazardous Materials Division, AXX-700; at the Washington Headquarters, the SSE is the Office of Internal Security, AIN-1.

4. **Where do I find more information about this order?**

- a. **Federal laws, regulations and guidance.** Appendix B
- b. **DOT and FAA orders and policies.** Appendix C
- c. **Summary of Protective Measures.** Appendix F

APPENDIX A. INFORMATION COMPRISING SENSITIVE SECURITY INFORMATION

Except as otherwise provided in writing by the Secretary of DOT in the interest of public safety or in furtherance of transportation security, the following information, and records containing such information, comprise Sensitive Security Information:

1. Security programs and contingency plans. Any security program or security contingency plan issued, established, required, received, or approved by any organizational element of the DOT or Department of Homeland Security (DHS), including:

- a. Any aircraft operator or airport operator security program or security contingency plan;
- b. Any vessel, maritime facility, or port area security plan required or directed under Federal law;
- c. Any national or area security plan prepared under 46 U.S.C. 70103; and
- d. Any security incident response plan established under 46 U.S.C. 70104.

2. Security Directives. Any Security Directive or order

- a. Issued by the Transportation Security Administration under 49 CFR 1542.303, 1544.305, or other authority;
- b. Issued by the Coast Guard under the Maritime Transportation Security Act, 33 CFR part 6, or 33 U.S.C. 1221 *et seq.* related to maritime security; or
- c. Any comments, instructions, and implementing guidance pertaining thereto.

3. Information Circulars. Any notice issued by the Department of Homeland Security or DOT regarding a threat to aviation or maritime transportation, including any

- a. Information Circular issued by the Transportation Security Administration under 49 CFR 1542.303 or 1544.305, or other authority; and
- b. Navigation or Vessel Inspection Circular issued by the Coast Guard related to maritime security.

4. Performance specifications. Any performance specification and any description of a test object or test procedure, for

- a. Any device used by the Federal government or any other person pursuant to any aviation or maritime transportation security requirements of Federal law for the detection of any weapon, explosive, incendiary, or destructive device or substance; and

b. Any communications equipment used by the Federal government or any other person in carrying out or complying with any aviation or maritime transportation security requirements of Federal law.

5. Vulnerability assessments. Any vulnerability assessment directed, created, held, funded, or approved by the DOT, Department of Homeland Security (DHS), or that will be provided to DOT or DHS in support of a Federal security program.

6. Security inspection or investigative information

a. Details of any security inspection or investigation of an alleged violation of aviation or maritime transportation security requirements of Federal law that could reveal a security vulnerability, including the identity of the Federal special agent or other Federal employee who conducted the inspection or audit.

b. In the case of inspections or investigations performed by the Transportation Security Administration (TSA), this includes the following information as to events that occurred within 12 months of the date of release of the information: the name of the airport where a violation occurred, the airport identifier in the case number, a description of the violation, the regulation allegedly violated, and the identity of any aircraft operator in connection with specific locations or specific security procedures. Such information will be released after the relevant 12-month period, except that TSA will not release the specific gate or other location on an airport where an event occurred, regardless of the amount of time that has passed since its occurrence. During the period within 12 months of the date of release of the information, TSA may release summaries of an aircraft operator's, but not an airport operator's, total security violations in a specified time range without identifying specific violations or locations. Summaries may include total enforcement actions, total proposed civil penalty amounts, number of cases opened, number of cases referred to TSA or FAA counsel for legal enforcement action, and number of cases closed.

7. Threat information Any information held by the Federal government concerning threats against transportation or transportation systems and sources and methods used to gather or develop threat information, including threats against cyber infrastructure.

8. Security measures. Specific details of aviation or maritime transportation security measures, both operational and technical, whether applied directly by the Federal government or another person, including

a. Security measures or protocols recommended by the Federal government;

b. Information concerning the deployments, numbers, and operations of Coast Guard personnel engaged in maritime security duties and Federal Air Marshals, to the extent it is not classified national security information; and

c. Information concerning the deployments and operations of Federal Flight Deck Officers, and numbers of Federal Flight Deck Officers aggregated by aircraft operator.

9. Security screening information. The following information regarding security screening under aviation or maritime transportation security requirements of Federal law:

a. Any procedures, including selection criteria and any comments, instructions, and implementing guidance pertaining thereto, for screening of persons, accessible property, checked baggage, U.S. mail, stores, and cargo, that is conducted by the Federal government or any other authorized person.

b. Information and sources of information used by a passenger or property screening program or system, including an automated screening system.

c. Detailed information about the locations at which particular screening methods or equipment are used, only if determined by the Transportation Security Administration to be Sensitive Security Information.

d. Any security screener test and scores of such tests.

e. Performance or testing data from security equipment or screening systems.

f. Any electronic image shown on any screening equipment monitor, including threat images and descriptions of threat images for threat image projection systems.

10. Security training materials. Records created or obtained for the purpose of training persons employed by, contracted with, or acting for the Federal government or another person to carry out any aviation or maritime transportation security measures required or recommended by the Department of Homeland Security or DOT.

11. Identifying information of certain transportation security personnel.

a. Lists of the names or other identifying information that identify persons as:

(1) Having unescorted access to a secure area of an airport or a secure or restricted area of a maritime facility, port area, or vessel or;

(2) Holding a position as a security screener employed by or under contract with the Federal government pursuant to transportation security requirements of Federal law, where such lists are aggregated by airport;

(3) Holding a position with the Coast Guard responsible for conducting vulnerability assessments, security boardings, or engaged in operations to enforce maritime security requirements or conduct force protection;

(4) Holding a position as a Federal Air Marshal; or

b. The name or other identifying information that identifies a person as a current, former, or applicant for Federal Flight Deck Officer.

12. Critical aviation or maritime infrastructure asset information. Any list identifying systems or assets, whether physical or virtual, so vital to the aviation or maritime transportation system that the incapacity or destruction of such assets would have a debilitating impact on transportation security, if the list is

- a. Prepared by any organizational element of the DOT or DHS; or
- b. Prepared by a State or local government agency and submitted by the agency to any organizational element of the DOT or DHS

13. Systems security information. Any security information for mission or administrative information systems operated by or for the Federal government that have been identified by the FAA, DOT, or DHS as critical to aviation safety and security. Systems security information includes vulnerabilities, security measures, and results of security assessments for those systems.

a. **Critical Infrastructure Systems.** The FAA Information System Security Handbook organizes FAA information systems into three tiers: Critical Infrastructure Systems, Essential Infrastructure Systems, and Other Systems. While all FAA systems security information is sensitive unclassified information (SUI), only systems security information for our Critical Infrastructure Systems is SSI.

b. **Essential Infrastructure and Other Systems.** For Official Use Only (FOUO) is the appropriate designation for systems security information relating to the FAA's other tiers:

- (1) Essential Infrastructure Systems and
- (2) Other Systems.

c. **FAA systems security information.** Our systems security information includes, but is not limited to, all documents associated with a system's Security Certification and Accreditation Package.

14. Confidential business information. *The bulk of procurement, grant, or confidential business information is not security information and does not constitute SSI.* You should protect confidential business information, *not related to transportation security*, as For Official Use Only (FOUO) information, unless the originator specifies other protective measures. Appendix F summarizes protective measures for FOUO information. Confidential business information is SSI when it deals with:

a. Solicited or unsolicited proposals received by the Department of Homeland Security or DOT, and negotiations arising there from, to perform work pursuant to a grant, contract, cooperative agreement, or other transaction, but only to the extent that the subject matter of the proposal relates to aviation or maritime transportation security measures;

b. Trade secret information, including information required or requested by regulation or Security Directive, obtained by DHS or DOT in carrying out aviation or maritime transportation security responsibilities; and

c. Commercial or financial information, including information required or requested by regulation or Security Directive, obtained by DHS or DOT in carrying out aviation or maritime transportation security responsibilities, but only if the source of the information does not customarily disclose it to the public.

15. Research and development. Information obtained or developed in the conduct of research related to aviation or maritime transportation security activities, where such research is approved, accepted, funded, recommended, or directed by the Department of Homeland Security or DOT, including research results.

16. Other information. Any information not otherwise described by 49 CFR Part 15.5 that the Secretary of DOT, FAA Administrator, or ASH-1 determines is SSI under 49 U.S.C. 40119. Upon the request of another Federal agency, the Secretary of DOT may designate as SSI information not otherwise described by 49 CFR Part 15.5.

APPENDIX B. FEDERAL LAWS, REGULATIONS, AND GUIDANCE

Sections 892 and 893, Public Law 107-296 - Homeland Security Act of 2002. This law and Executive Order 13311 establish United States Government policy and procedures for sharing sensitive homeland security information.

44 U.S.C. Chapter 35, Coordination of Federal Information Policy. This law ensures that creating, collecting, maintaining, using, disseminating, and disposing of information by or for the Federal Government is consistent with applicable laws, including laws relating to privacy and confidentiality, security of information, and access to information.

49 U.S.C § 40119. This law establishes the authority of the Department of Transportation and the Department of Homeland Security to protect information developed during security activities.

Title III of Public Law 107-347 - The Federal Information Security Management Act of 2002. This act provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets.

6 CFR Part 29, Procedures for Handling Critical Infrastructure Information; Interim Rule. This rule establishes procedures to implement section 214 of the Homeland Security Act of 2002 regarding the receipt, care, and storage critical infrastructure information voluntarily submitted to the Department of Homeland Security.

49 CFR Parts 15 & 1520, Protection of Sensitive Security Information. These regulations, issued jointly by DOT and the Department of Homeland Security, regulate the release of records and information obtained or developed during security activities.

Homeland Security Presidential Directive/Hspd-7, Critical Infrastructure Identification, Prioritization, and Protection. This directive establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks.

Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems. This document establishes standards for security categorization of Federal information and information systems under the E-Government Act of 2002.

National Institute of Standards and Technology (NIST) Special Publication 800-60, Volumes I and II: Guide for Mapping Types of Information and Information Systems to Security Categories. These guides help Federal agencies identify types of SUI and determine potential impact if we disclose SUI to unauthorized persons.

APPENDIX C. DOT AND FAA ORDERS AND POLICIES

DOT Order 1640.4, Chapter 5, For Official Use Only Information (FOUO). Chapter 5 discusses the purpose of FOUO information and its marking and safeguarding.

FAA Order 1270.1, Freedom of Information Act (FOIA) Program. This order provides direction and administration of the FOIA at all levels within the FAA.

FAA Order 1280.1, Protecting Privacy of Information about Individuals. This order implements the Privacy Act of 1974, as amended, within the FAA.

FAA Order 1370.79, Internet Use Policy. This order establishes agency-wide policy on the appropriate use of the Internet, which includes unauthorized disclosure of sensitive information.

FAA Order 1370.81, Electronic Mail. This order establishes agency-wide policy on the use, operation, and management of the FAA's electronic mail system.

FAA Order 1370.82, Information Systems Security Program. This order establishes policy and assigns responsibilities to implement national and DOT security policies for FAA information systems. It applies to all FAA information (including classified) collected, stored, processed, disseminated, or transmitted using FAA or non-FAA information systems.

FAA Order 1600.2, Safeguarding Controls and Procedures for Classified National Security Information and Sensitive Unclassified Information. This order implements Executive Order 12958, as amended, within the FAA.

FAA Order 1600.73, Contractor and Industrial Security Program Operating Procedures. This order establishes procedures for the FAA's Contractor and Industrial Security Program.

FAA Order 1600.74, Visitor Procedures for Federal Aviation Administration Facilities. This order establishes policy for allowing visitors access to FAA facilities.

FAA Human Resources Policy Manual, ER 4-1, Standards of Conduct. This directive establishes the standards of conduct for FAA employees, including conduct standards for safeguarding and handling government information.

FAA Acquisition System Toolset (FAST), <http://fast.faa.gov>. FAST addresses procurement policy and procedures to include SUI in contracts.

FAA Telecommuting Handbook of May 1997. This handbook addresses the basic policy framework for protecting SUI while telecommuting.

APPENDIX D. MARKING FOUO INFORMATION



U.S. Department
of Transportation
**Federal Aviation
Administration**

Memorandum

Subject:	Marking FOR OFFICIAL USE ONLY (FOUO) Documents	Date:	
From:		Reply to Attn. of:	
To:			

This document is marked for instructional purposes only. It contains no FOUO information.

You must mark FOUO documents **“FOR OFFICIAL USE ONLY”**, font size 12 or greater in bold capital letters, and **“Public availability to be determined under 5 USC 552”** at the bottom of the

- front cover,
- first page, and
- outside back cover

If your document has multiple pages, mark each page containing FOUO information **“FOR OFFICIAL USE ONLY”** at the bottom of page.

When sending FOUO material outside the DOT, your transmittal record should include a statement like this:

This document/record belongs to the Federal Aviation Administration and may be used for official Government purposes only. It may not be released without the expressed permission of the Federal Aviation Administration. Refer requests for the document to: (insert name and address of originating office.)

FOR OFFICIAL USE ONLY

Public availability to be determined under 5 USC 552

APPENDIX E. MARKING SENSITIVE SECURITY INFORMATION

SENSITIVE SECURITY INFORMATION



U.S. Department
of Transportation
**Federal Aviation
Administration**

Memorandum

Subject:	Marking SENSITIVE SECURITY INFORMATION (SSI) Documents	Date:	
From:		Reply to Attn. of:	
To:			

This document is marked for instructional purposes only. It contains no SSI.

Note: 49 CFR § 15.5 and Appendix A list information that constitute SSI and that may be marked SSI. You do not need to remark SSI designated under prior authorities, 14 CFR § 191 and 49 CFR § 1520 of February 22, 2002.

In the case of paper records containing SSI, place:

1. The protective marking “**SENSITIVE SECURITY INFORMATION**”, font size 12 or higher in bold capital letters, on the top of the outside of any front and back cover, including a binder cover or folder, if the document has a front and back cover; any title page; and each page of the document.
2. The distribution limitation statement, that appears below, on the bottom of the outside of any front and back cover, including a binder cover or folder, if the document has a front and back cover, any title page; and each page of the document.

Other types of records. In the case of non-paper records that contain SSI, including motion picture films, photography, videotape recordings, audio recordings, electronic and magnetic records, and removable electronic media, a covered person must clearly and conspicuously mark the record with the protective marking and the distribution limitation statement such that the viewer or listener is reasonably likely to see or hear them when accessing the records.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

APPENDIX F. SUMMARY OF PROTECTIVE MEASURES

Minimum Protective Measures				
● Required Protective Measure ■ Not applicable	FOUO	SSI	SHSI	PCII
Access – Restricted to persons who have a <i>duty to protect</i> and <i>need-to-know</i> . Chapter 2, para 2 & 3 this order	●	-	-	-
Access – Restricted to <i>covered persons</i> as defined by 49 CFR § 15.7 and persons with need-to-know as defined by 49 CFR § 15.11. Chapter 2, para 2.b this order	-	●	-	-
Access – Restricted to Federal agencies and appropriated State and local persons for the purpose of predicting, analyzing, investigating, deterring, preventing, protecting against, mitigating the effects of, or recovering from the acts of terrorism. § 892 HSA of 2002, Hspd-7, Chapter 2, para 2.c, this order	-	-	●	-
Access – Restricted by 6 CFR § 29.8	-	-	-	●
FOIA - FOIA exemption 3 may apply. 49 CFR § 15.15(a); § 892 HSA of 2002; 6 CFR § 29.8(g)	-	●	●	●
FOIA – FOIA exemptions 2 through 9 may apply. FAA Order 1270.1	●	-	-	-
Duration of protection – No longer then required to protect information sensitivity. Chapter 3, para 19 this order & 49 CFR § 15.5(c)	●	●	●	-
Duration of protection – No longer then 5 years unless warranted for a longer period.	-	-	●	-
Duration of protection – Until changed by the Protect CII Program Manager or this manager's designee. 6 CFR § 29.6(b)	-	-	-	●
Penalties - Criminal or Administrative penalties for unauthorized disclosure. Chapter 2, para 5 this order; 49 CFR § 15.17; 6 CFR § 29.9(d)	●	●	●	●
Record accountability - Document & material tracking. 6 CFR § 29.6(d)	-	-	-	●
Marking documents – Distribution limitation statement or warning notice. Appendices D & E this order; 6 CFR § 29.6(c); 49 CFR § 15.13	●	●	●	●
Marking documents – Protective markings. Chapter 3, para 3-6, and Appendices D & E of this order; FAA Order 1370.81A; 6 CFR § 29.5(a); 49 CFR § 15.13	●	●	●	●
Marking other materials – Place protective markings and distribution limitation statements or warning notices so that the viewer or listener is reasonably likely to see or hear the markings and statement when they access the record. Chapter 3, para 6 this order; 49 CFR § 15.13(d)	●	●	●	●

Minimum Protective Measures				
● Required Protective Measure ■ Not applicable	FOUO	SSI	SHSI	PCII
When in physical possession of a person - Take reasonable steps to safeguard and protect the information so that is not disclosed to unauthorized persons. Chapter 1, para 11.d and chapter 3, para 9.f, this order; 49 CFR § 15.9(a); 6 CFR § 29.7(a)	●	●	●	●
Storage – When not in physical possession of a person, store in a locked security container, desk, file cabinet, or space. Store by means that affords the information protection appropriate to its vulnerability and sensitivity. Chapter 3 para 7 & 8 this order; 49 CFR § 15.9(a); 6 CFR § 29.7(b)	●	●	●	●
Automated Information System (AIS) Security - Electronic and email transmission over the Internet: protect with FIPS approved encryption. Chapter 3, para 15 this order; FAA Order 1370.81A; 6 CFR § 29.7(e)&(f)	●	●	●	●
AIS Security - May not post on or provide access from a publicly accessible website or electronic portal. Chapter 3, para 16, this order; FAA Orders 1370.79A & 1370.82	●	●	●	●
Contractor access – Include protection requirements in the contract, grant, or licensing agreement or separate non-disclosure agreement. Chapter 1, para 11.c.(4), and chapter 2, para 2, this order; FAA Order 1370.82; 6 CFR § 29.8(c); FAA Acquisition Management System policy	●	●	●	●
Reproduction - To extent needed to carry out official duties. Mark and protect copies in the same manner as the originals. Chapter 3, para 9 this order	●	●	●	●
Destruction of paper records - Destroy so recovery is difficult. Minimum – hand tear or shred in small pieces and mix with other wastepaper material. Chapter 3, para 17 this order	●	■	■	■
Destruction of paper records - Destroy by shredding, burning, pulping, pulverizing, or some other method that assures destruction beyond recognition and reconstruction. Chapter 3, para 17 this order	■	●	●	●
Destruction of electronic media - Clear, sanitize, or destroy by approved means. Chapter 3, para 18, this order; FAA Order 1370.82	●	●	●	●
Automated information system – Certification and accreditation based on risk. FAA Order 1370.82	●	●	●	●
Reporting - Report unauthorized disclosure. Chapter 1, para 11.c.(8), and chapter 2, para 4, this order	●	●	●	●

RECORD OF CHANGES

DIRECTIVE NO.

1600.75

[illegible]