ORDER

1280.1A

PROTECTING PRIVACY OF INFORMATION ABOUT INDIVIDUALS

October 7, 1994

DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION

Distribution: A-WXYZ-2; A-FOF-O (LTD); A-E-1

Initiated By: AIT-400

RECORD OF CHANGES

DIRECTIVE NO. 1280.1A

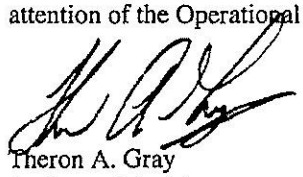
CHANGE TO BASIC	SUPPLEMENTS			OPTIONAL	CHANGE TO BASIC	SUPPLEMENTS			OPTIONAL

FOREWORD

This order provides for the administration of the Privacy Act of 1974, as amended, within FAA. It states the authorities, requirements, and responsibilities for administering the Privacy Act.

The material in this order provides direction for the administration of the Privacy Act at all levels within FAA. However, questions and problems could arise which may not be specifically addressed in the order. The heads of offices and services in Washington headquarters, and the administrators of the regions and centers are required to designate a Privacy Act Coordinator. Problems and questions should be directed to that individual who should, in turn, seek the assistance of the Operational Privacy Act Coordinator in the Office of the Assistant Administrator for Information Technology, AIT-400.

This revision updates references and adds new guidance on matching programs. The contents have been prepared on an agencywide basis; therefore, individual organizations may supplement this broad coverage with specific guidelines and instructions specific to their needs. Supplementation which may have agencywide application should be brought to the attention of the Operational Privacy Act Coordinator, AIT-400.



Theron A. Gray
Assistant Administrator
for Information Technology

TABLE OF CONTENTS

CHAPTER 1. GENERAL **1**

SECTION 1. INTRODUCTION 1
1-1. Purpose. 1
1-2. Distribution. 1
1-3. Cancellation. 1
1-4. Background. 1
1-5. Explanation Of Changes. 1
1-6. Delegation Of Authority. 1
1-7. Definitions. 2
1-8. Forms And Reports 3
SECTION 2. REQUIREMENTS AND RESPONSIBILITIES 3
1-9. Requirements. 3
1-10. Responsibilities. 4

CHAPTER 2. DISCLOSURE AND ACCESS OF RECORDS **11**

SECTION 1. GENERAL 11
2-1. Conditions Of Disclosure. 11
2-2. Records Originated Outside FAA 11
2-3. Access To Records. 12
SECTION 2. HANDLING REQUESTS FOR RECORDS AND CORRECTIONS 13
2-4. Mail Requests From Individuals For Records Pertaining To Themselves. 13
2-5. In-Person Requests From Individuals For Records Pertaining To Themselves. 13
2-6. Third Party Requests. 14
2-7. Corrections To Records. 14
SECTION 3. APPEALS 15
2-8. Advising Requester Of Rights To Appeal. 15
2-9. Internal FAA Appeals Procedures. 15
SECTION 4. CIVIL REMEDIES 16
2-10. Description Of Circumstances. 16
2-11. Judicial Review Of Agency's Refusal To Amend A Record. 16
2-12. Judicial Review Of Agency's Denial Of Access To A Record. 17
2-13. Judicial Review Of Agency's Failure To Maintain A Record Properly. 17
2-14. Judicial Review Of Other Failures Of The Agency To Comply With The Act. 17
SECTION 5. CRIMINAL PENALTIES 17
2-15. Penalties. 17
SECTION 6. FEES 18
2-16. When To Charge Fees. 18

CHAPTER 3. COLLECTION AND MAINTENANCE OF SYSTEMS OF RECORDS **23**

3-1. General Statement. 23
3-2. Procedures For Collecting Information. 23
3-3. Maintenance Of Records. 24
3-4. Records Made Available Under Compulsory Legal Process. 24
3-5. Records Involved In Computerized Matching Programs. 24
3-6. Records Safeguards. 25
3-7. Transfer Of Records. 25
3-8. Accounting Of Certain Disclosures. 25

CHAPTER 4. PERSONNEL RECORDS **31**

SECTION 1. GENERAL 31
4-1. Coverage 31
4-2. Changes. 31
4-3. Definitions. 31
4-4. Responsibilities Of The Personnel Privacy Act Officer. 31
4-5. Office Of Personnel Management (OPM) Regulations. 31
4-6. OPM/GOVT Systems Notices 31
SECTION 2. DISCLOSURE OF PERSONNEL RECORDS 32
4-7. Conditions Of Disclosure. 32
4-9. Disclosures Within FAA 33
SECTION 3. ACCESS TO AND CORRECTION OF PERSONNEL RECORDS AND PRIVACY ACT INQUIRIES 33
4-10. General. 33
4-11. Grant Of Access. 33
4-12. Denial Of Access. 34
4-13. Requests For Amendment Of Or Correction To Personnel Records. 34
4-14. FAA Initiated Amendment Or Correction Of Personnel Records. 36
4-15. Privacy Act Inquiries. 36
SECTION 4. COLLECTION AND MAINTENANCE OF PERSONNEL RECORDS 37
4-16. Written Explanations 37
4-17. Standards Of Accuracy For Personnel Records. 37
4-18. Annual Review Announcement. 37
4-19. Safeguarding Personnel Records. 37
SECTION 5. MISCELLANEOUS PROVISIONS 37
4-20. Specific Personnel Records. 37
4-21. Confidential Employment Inquiries (Vouchers). 38
4-22. Reference Inquiries Received. 38
4-23. Privacy Act Statement For MPP Announcements. 38
4-24. Responding To Congressional Inquiries. 38
4-25. Fees. 39
4-26. Leave Charts. 39
4-27. Personnel Management Information System (PMIS). 39
SECTION 6. SUPERVISOR'S PERSONNEL RECORDS 39
4-28. Authorized Supervisor's Personnel Records. 39
4-29. Guidance For Supervisors. 40
4-30. Uncirculated Personal Notes. 40

CHAPTER 5. SAFEGUARDING PRIVACY ACT RECORDS **46**

SECTION 1. GENERAL 47
5-1. Privacy Act Security Requirements. 47
5-2. Safeguard Selection. 47
5-3. Security Risk Assessment. 47
5-4 Inspections. 47
SECTION 2. PROTECTION OF MANUAL RECORDS SYSTEMS 48
5-5. Introduction. 48
5-6. Required Safeguards. 48
5-7. Identifying Personnel Authorized Access. 49
5-8. Local Security Plan Checklist. 49
5-9. Key Control. 50
SECTION 3. SAFEGUARDING AUTOMATED RECORDS 50
5-10. General. 50
5-11. Physical Security. 50
5-12. Information Management Practices. 50

5-13. System And Network Safeguards. 51
5-14. New Systems Or Major Changes To Existing Systems. 51

CHAPTER 6. EXEMPTIONS AND SPECIAL SITUATIONS 54

6-1. General Exemptions. 55
6-2. Special Exemptions. 55
6-3. Procedures For Exempting Systems Of Records. 55
6-4. Government Contractors 55
6-5. Statistical Records. 55

CHAPTER 7. REPORTS 57

7-1. New Or Revised Systems Of Records (RIS: 1280-3). 57
7-2. Cancellation Of Systems Of Records. 57
7-3. Privacy Act Statistical Summary (RIS: 1280-2). 57

APPENDIX 1. FEES 1

APPENDIX 2. INDEX 1

CHAPTER 1. GENERAL

SECTION 1. Introduction

1-1. PURPOSE.

This order implements within the FAA, the Privacy Act of 1974, as amended by the Computer Matching and Privacy Protection Act of 1988; supplements the guidance provided by the Office of Management and Budget (OMB) and the Office of the Secretary of Transportation (OST); and provides instructions and guidance to all FAA elements to assist them in implementing the provisions of the Act. It implements the provisions of DOT H 1350.2 Departmental Information Resources Management Manual (DIRMM).

1-2. DISTRIBUTION.

This order is distributed to the division level in Washington, regions, and centers; and limited distribution to each field office and facility and resident directors in the Western-Pacific Region.

1-3. CANCELLATION.

Order 1280.1, Protecting Privacy of Information About Individuals, dated September 8, 1989, is canceled.

1-4. BACKGROUND.

The Congress of the United States found that the privacy of individuals has been endangered by the increasing use of computers and sophisticated information collecting and disseminating technology by Federal agencies in their conduct of the affairs of Government. The Act provides specific safeguards for individuals against unwarranted invasions of privacy by requiring all Federal agencies to adhere to certain standards for collecting, maintaining, using, and/or disseminating information of a personal nature about individuals.

1-5. EXPLANATION OF CHANGES.

a. Changes to routing symbols and titles

b. Changes to Chapter 3 to include process for approval of computer matching programs.

c. Removal of appendix 2, OMB Guidelines for Performing Matching Programs, of Order 1280.1.

d. Changes the work flow/responsibilities in the FAA internal appeal process to show the Office of the Chief Counsel, General Law Branch, AGC-110, responsibilities.

e. Changes to chapter 5, including new guidance on the use of fax machines and electronic mail.

f. Changes to chapter 7 to include the new procedures for the biennial statistical report.

g. Clarified references to supervision one level above system manager.

h. Added reference to the signatory authority of the regional administrators.

1-6. DELEGATION OF AUTHORITY.

a. **System managers assigned** responsibility for systems of records and identified in the public notice issued pursuant to the Act, as a further exercise of that responsibility, will:

(1) Grant access to FAA records to the individuals to whom the records pertain.

(2) Deny access to FAA records to individuals to whom the records pertain only if such denial is justified under a published general or specific exemption from the access requirements of the Act, or if the records were compiled in reasonable anticipation of a civil action or proceeding.

(3) Amend FAA records on the basis of a substantiated request for amendment by the individual to whom the records pertain.

(4) Permit disclosure of records, if authorized under paragraph 2-1 of chapter 2.

(5) Prior to completing a determination to deny an individual access to or right to amend his/her records, the system manager will coordinate the decision with the appropriate Privacy Act Coordinator and obtain concurrence from legal counsel; i.e., regional and center Assistant Chief Counsels, and in Washington Headquarters, with the Office of the Chief Counsel.

NOTE: If the system manager is below the division level or equivalent, the supervisor at the division level or above will, after consultation with legal counsel, make the final determination.

b. **Regional Administrators.** In accordance with the current version of FAA Order 1100.154, paragraph 7-1, regional administrators have signatory authority for administrative matters which cross program lines. As part of that authority, the regional administrators may sign denials under the Privacy Act, or delegate that responsibility to a lower level, including the division manager where the system resides.

c. **The Assistant Administrator for Information Technology, AIT-1,** after consultation with the Chief Counsel, will make final agency determinations on appeals. This authority may only be exercised by the Administrator, Deputy Administrator, Executive Director or Assistant Administrator for Information Technology. The exception to this rule is in connection with personnel records. The Office of Personnel Management (OPM) will make final determinations in these cases.

d. **The Assistant Administrator for Information Technology, AIT-1,** will chair the FAA Data Integrity Review Committee responsible for reviewing Privacy Act computer matching programs.

e. **The Manager, IT Information Management Division, AIT-400,** may extend, if necessary, the 30-working day period for processing final determinations on agency refusals to amend or deny access to records.

1-7. DEFINITIONS.

These definitions and those contained in paragraph 4-3 apply to the implementation of the Privacy Act.

a. **Agency** includes any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency. For purposes of the Privacy Act, DOT is considered as a single agency.

b. **Confidentiality** is a concept that applies to information. It is the state afforded to information which requires protection against unauthorized disclosure.

c. **The Data Integrity Board** is a board established in compliance with the Computer Matching and Privacy Protection Act of 1988. This board reviews and approves or disapproves computer matching programs if the Department of Transportation is either a source or recipient (or matching) agency.

d. **The FAA Data Integrity Review Committee** reviews all computer matching programs the agency proposes to conduct with other agencies or state or local governments. This committee reviews these computer matching programs before the proposed programs are brought before the Departmental Data Integrity Board. The FAA Committee consists of AIT-1 as chair, AGC-110, and AIT-400 as secretary.

e. **Disclosure** means the divulging of information by any means of communication of a record contained in a Privacy Act system of records to any person or to another agency other than the individual to whom the information pertains. This includes the transfer of a record or the granting of access to a record.

f. **FAA Privacy Act Coordinator** refers to the Manager, IT Information Management Division, AIT-400, who is responsible for the implementation and management of the Privacy Act within FAA.

g. **Individual** means a citizen of the United States or an alien lawfully admitted for permanent residence. A proprietorship or any collection of individuals; e.g., corporations, partnerships, etc., are not considered individuals for purposes of this order.

h. **Integrity** is the state existing when data agrees with the source from which it is derived; and when it has not been either accidentally or maliciously altered, disclosed, or destroyed.

i. **Maintain** includes maintain, collect, use, or disseminate, and is used in two ways in the Privacy Act. First, it is used to connote the various record keeping functions to which the requirements of the Act apply; second, it is used to connote control over and hence responsibility and accountability for systems of records.

j. **Matching programs** mean any computerized comparison of two or more automated systems of records or a system of records with non-Federal records.

k. **Officers and Employees** mean all persons employed by the FAA in any capacity, and also includes any person authorized by FAA, to operate or maintain, on behalf of the FAA, a system of records necessary to accomplish an FAA function.

l. **Operational Privacy Act Coordinator** refers to the individual designated by the FAA Privacy Act Coordinator, AIT-400, to conduct and maintain the Privacy Act program within FAA.

m. **Personnel Record** means any personal information maintained in a system of records that is needed at any echelon of management for personnel management programs or processes such as staffing, employee development, retirement, grievances and appeals, etc. The categories of records are described in Systems of Records Notices which are published annually in the Federal Register. Privacy Act Coordinators should retain a copy of the current publication. (For further explanation, see chapter 4.)

n. **Privacy Act Coordinator** refers to an individual who has Privacy Act responsibilities within an organizational or geographic element of the FAA; i.e., Washington Headquarters offices/services and regions and centers. That individual would be the contact point for the Operational Privacy Act Coordinator.

o. **Record** means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his/her education, financial transactions, medical history, and criminal or em-

ployment history, and that contains his/her name, or identifying number, symbol, or other identifying particular assigned to an individual, such as a fingerprint, voiceprint, or photograph.

p. Request for Access means a request by an individual or other authorized person to review, and receive a copy if requested, a record which is in a particular system of records which pertains to that individual.

q. Routine Use means, with respect to the disclosure of a record, a use which is compatible with the purpose for which the record was collected. Routine uses for each DOT/FAA system of records are published in the Federal Register.

r. Security is the protection afforded information from accidental or intentional but unauthorized modification, destruction, or disclosure.

s. Statistical Record means a record in a system of records maintained for statistical research or reporting purposes only, and not used in whole or in part in making any determinations about an identifiable individual, except as provided in section 8 of Title 13, U.S.C. (Title 13 U.S.C. concerns the Bureau of the Census)

t. System Manager refers to the person responsible for the collection, use, maintenance, and dissemination of information pertaining to individuals contained in systems of records. The system manager does not have to have physical custody of the records; he or she must, however, be in position to exercise effective control over the system of records. System managers for each DOT/FAA system of records are identified in the System of Records Notice published in the Federal Register.

u. System of Records means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

NOTE: The "are retrieved by" criterion implies that the grouping of records under the control of an agency is accessed by the agency by use of a personal identifier; not merely that a capability or potential for retrieval exists. (OMB guidelines)

v. Unauthorized Person refers to any individual who has not established a need, in the performance of his or her duties, for access to any record within a system of records. The system manager of the concerned system of records determines whether the criteria for access is met.

1-8. FORMS AND REPORTS.

The following forms and reports are prescribed for use in the system:

a. Forms Listings.

(1) FAA Form 1300-11, History, NSN 0052-00-808-9000, Unit of Issue: Sheet. (See paragraph 3-8 b(2))

(2) FAA Form 1280-1, Privacy Statistical Disclosure Summary, NSN 0052-00-915-8000, Unit of Issue: Sheet. (See paragraph 7-3)

b. Reports Listings.

(1) Privacy Act Statistical Summary (RIS 1280-2) (See paragraph 7-3)

(2) New or Revised Systems of Records (RIS: 1280-3) (See paragraph 7-1)

SECTION 2. REQUIREMENTS AND RESPONSIBILITIES

1-9. REQUIREMENTS.

a. Any information in a system of records shall not be disclosed to any person or to another agency except with the prior written consent of the individual to whom the record pertains, unless the disclosure is authorized under paragraph 2-1 of chapter 2, Conditions of Disclosure.

b. An individual shall be permitted to review and have a copy of all or any portion of the agency records which pertain to him/her (except for those records compiled in reasonable anticipation of a civil action or proceeding, or those records exempted from the access requirements of the Act and published as general or specific exemptions. (See chapter 6)) The individual may also request amendments to those records if he/she believes the information is not totally accurate, relevant, timely, or complete.

c. Only that information which is considered relevant and necessary to accomplish a purpose of the FAA, or required by statute or Executive Order shall be collected and maintained. To the greatest extent possible, such information shall be collected directly from the individual when the information may result in adverse determinations about his or her rights, benefits, and privileges under Federal Government programs.

d. All requests by individuals to review or copy records will be handled in an efficient and expeditious manner. Every effort will be made to assist individuals in getting their requests for records to the appropriate location.

e. The Privacy Act, unlike the Freedom of Information Act (FOIA), is mainly concerned with protecting the individual's right to privacy. It cannot be used, however, to deny to the public that information in systems of records

which is required to be disclosed under FOIA. The procedures outlined in this order are designed to assist FAA officers and employees who are responsible for maintaining, collecting, using, and disseminating personal information. These individuals should become equally familiar with Order 1200.23, Public Availability of Information.

f. Controls will be established to ensure that the safeguard requirements of the Privacy Act are met through the application of appropriate physical, technical, and administrative controls in both manual and automated record systems. The objective of these controls is to ensure the security, confidentiality, and integrity of personal information held by all FAA components.

g. Individuals from whom personal information is requested in connection with agency programs will be informed, at the time of the request, of the authority which authorizes the solicitation of the information and whether providing such information is mandatory or voluntary; the principal purposes for which the information is intended to be used; the routine uses which may be made of the information; and the effects, if any, of not providing all or any part of the requested information. The notification to the individual is done as a statement on the form used for collecting the information, or on a separate sheet handed to the individual at the time the information is collected. (See paragraph 3-2a)

h. Individuals will not be denied any right, benefit, or privilege provided by law because of the individual's refusal to provide his or her Social Security Number (SSN) UNLESS the disclosure of the SSN is required by Federal statute or regulation adopted prior to January 1, 1975, to verify the identity of the individual. (See paragraph 3-2b)

i. Other existing agency orders, notices, instructions, etc., containing specific criteria for obtaining or disseminating information about individuals should be followed so long as the provisions of the Privacy Act as described herein are not violated. Any inconsistencies noted should be brought to the attention of the IT Information Management Division, AIT-400.

1-10. RESPONSIBILITIES.

a. The Manager of the IT Information Management Division, AIT-400, as the FAA Privacy Act Coordinator, is responsible for the implementation and administration of the Privacy Act throughout FAA, including serving or designating someone to serve on the FAA Data Integrity Review Committee.

b. The Manager, IT Information Management Division, AIT-400, shall designate an Operational Privacy Act Coordinator who is responsible for:

(1) Conducting and maintaining the Privacy Act Program in FAA.

(2) Assisting Privacy Act Coordinators, systems managers, and other officers and employees of the FAA in the conduct and disposition of the operational aspects of the Privacy Act Program.

(3) Serving as the point of contact within FAA and the focal point for submission of reports and Privacy Act information to OST, OMB, Congress, and others as required.

(4) Ensuring coordination of all rules and other notices required by the Privacy Act to be published by the FAA in the Federal Register.

(5) Providing Privacy Act Coordinators with copies of each notice or change of systems of records affecting FAA that appear in the Federal Register.

(6) Serve on the FAA Data Integrity Review Committee.

c. The Assistant Administrator for Information Technology, AIT-1, has the final agency responsibility for Privacy Act appeal decisions unless AIT-1 is a party to the appeal, in which case the Administrator or designee is the final authority.

d. The Office of the Chief Counsel is responsible for providing assistance to AIT-1 and AIT-400 with respect to the resolution within FAA of all legal matters relating to the Act, including interpretations of the letter and spirit of the Act, legal drafting necessary to implement the Act, and coordinating with the General Counsel in OST, all final determinations to deny access or to amend records. The Chief Counsel, AGC-1, or designee will serve on the FAA Data Integrity Review Committee.

e. The Chief Counsel and Regional and Center Assistant Chief Counsels are responsible for providing legal assistance to:

(1) System managers,

(2) Reviewing officials,

(3) Privacy Act Coordinators, and

(4) Other employees and officers within their respective geographic or organizational jurisdictions in exercising their responsibilities under the Act.

f. The Assistant Administrator for Civil Aviation Security, ACS-1, is responsible for:

(1) Functioning as the FAA Privacy Act Security Officer and as a part of that responsibility will:

(a) Support the FAA Privacy Act Coordinator by establishing the security policies required to comply with the safeguard requirements of the Privacy Act, and

(b) Handle all requests for release of classified information.

(2) Provide additional support and assistance upon request to the FAA Privacy Act Coordinator. Center and regional security component managers will function in a similar support and assistance capacity for their respective organizations.

g. System managers are responsible for:

(1) Maintaining the systems of records under their control in a manner consistent with the letter and spirit of the Privacy Act. These responsibilities include, but are not limited to, the following specific activities, whether they are performed by the system manager personally or by others acting under his or her direction:

(a) Receiving and processing requests for FAA records from persons to whom the records pertain, and ensuring the proper identity of requesters and their entitlement to the requested information.

(b) Receiving and processing requests from individuals to amend records pertaining to them.

(c) Providing facilities and services for inspecting and copying records.

(d) Collecting fees and charges for copying and certifying records in accordance with Part 10 of DOT Regulations, or 5 CFR Part 294, and for disposition of fees in accordance with applicable provisions of the current version of Order 2770.5, Collections - Receipt and Control.

(e) Preparing required reports concerning the system(s) of records as required by the FAA Operational Privacy Act Coordinator or other designated officials and as prescribed in chapters 3 and 7.

(f) Ensuring that the published Privacy Act system notice is accurate, and initiating action to update the notice when necessary.

(2) Ensuring that all employees who have access to the records contained in the system(s) of records are:

(a) Made fully aware of their responsibilities with respect to the protection of the subject information.

(b) Fully informed of the FAA access and disclosure policies and procedures.

(c) Personally aware of their individual responsibilities, including possible personal criminal liability, with respect to their handling of personal information to which they may have access.

(3) Complying with the record safeguarding requirements for material under their control.

h. Offices, services, regions, and centers are responsible for implementation and administration of the Privacy Act within their jurisdictions and for designating Privacy Act Coordinators to assist them.

i. Privacy Act Coordinators are responsible for:

(1) Coordinating the administration of the Privacy Act within their respective jurisdictions.

(2) Maintaining a current file of necessary systems notices.

(3) Ensuring the availability of appropriate training to employees within their respective jurisdictions on the Act and their responsibilities for the proper handling of personal data.

(4) Serving as the communication channel and providing staff advice and assistance within their respective jurisdictions with respect to individual and/or employee inquiries regarding systems of records, delegated authorities, and FAA procedures.

(5) Complying with requests from the FAA Operational Privacy Act Coordinator for information and data.

(6) Submitting information to the FAA Operational Privacy Act Coordinator on any new use or intended use of the information in a system of records.

(7) Complying with any other information requirements established by the Act or this order or requested by the FAA Operational Privacy Act Coordinator.

(8) Evaluating the application of Privacy Act policies and procedures within their respective jurisdictions.

j. All FAA officials and employees having agency responsibilities for collecting, maintaining, using, or disseminating systems of records which contain individually identifiable information are responsible for complying with the provisions of the Act.

k. All employees engaged in the design, development, operation, or maintenance of any system of records have a personal responsibility for adhering to the spirit and intent of the Act even though they might not be held accountable in terms of civil or criminal liability.

CHAPTER 2. DISCLOSURE AND ACCESS OF RECORDS

SECTION 1. GENERAL

2-1. CONDITIONS OF DISCLOSURE.

The Privacy Act's requirements on disclosure of records are stated in paragraph 1-9a. With respect to the disclosure of a record to a person or organization (government or private sector) other than the individual to whom the record pertains, the prior written consent of the subject individual is usually required. However, disclosures under any of the following conditions do not require the individual's prior written consent:

a. Disclosure to DOT officers and employees who have established a need for the record in the performance of their duties.

b. Disclosure of information which would be required to be released under the FOIA. If, under the FOIA, the requested information is not required to be disclosed, the consent of the individual must be obtained prior to disclosure unless the disclosure is permitted under one of the other conditions listed herein.

c. Disclosure for a routine use, as defined in chapter 1, provided the routine use has been established and described in the public notice required by the Act to be published in the Federal Register.

d. Disclosure to the Bureau of Census for purposes of planning or carrying out a lawfully constituted census, survey, or related activity.

e. Disclosure to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable. (See paragraph 6-5, Statistical Records)

f. Disclosure to the National Archives and Records Administration as a record which has sufficient historical or other value as to warrant its continued preservation by the United States Government, or for evaluation by the Archivist of the United States or his/her designee to determine if the record has such value.

g. Disclosure to another agency or to an instrumentality of any Governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity authorized by law, and if the head of the agency or instrumentality or his/her designee has made a written request to FAA specifying the particular portion of the record desired and the law enforcement activity for which the record is sought.

h. Disclosure to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure, notification is transmitted to the last known address of such individual. FAA may disclose records when the time required to obtain the consent of the individual to whom the record pertains might result in a delay which could impair the health or safety of an individual, as in the release of medical records on a patient undergoing emergency treatment. The individual to whom the records pertain need not necessarily be the individual whose health or safety is at peril; e.g., release of dental records on several individuals in order to identify an individual who was injured in an accident.

i. Disclosure to either House of Congress or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress, or subcommittee of any such joint committee.

j. Disclosure to the Comptroller General, or any authorized representatives, in the course of the performance of the duties of the General Accounting Office.

k. Disclosure pursuant to the order of a court of competent jurisdiction.

l. Disclosure to a consumer reporting agency in accordance with 31 U.S.C., section 3711(f).

2-2. RECORDS ORIGINATED OUTSIDE FAA.

When a requested record was not originated by FAA but rather by another element in DOT or by another Federal agency (although contained in a system of records maintained by FAA), the system manager shall:

a. Ensure that the originating organization has not exempted the record, and if it has not, make it available to the requester and advise the originating organization of the release of the information.

b. Forward a copy of the request to the originating agency for handling of its documents if the record has been exempted from particular provisions of the Act, and notify the requester of the action taken. The notification should include a contact person and phone number. The FAA, however, remains responsible for ensuring a response.

c. Treat records given to the FAA by State or local governments or private industry as FAA records unless it is clear on the document that the originating organization still maintains control over the document. In that case, consulta-

tion with the originating organization is required before notification or release of the information takes place.

2-3. ACCESS TO RECORDS.

a. Upon request by an individual to gain access to his/her record or to any information pertaining to him/her which is contained in a system of records, the FAA shall:

(1) Determine whether the current version of the request should be handled under FOIA or Privacy Act procedures. (If FOIA procedures are to be employed, see Order 1200.23, Public Availability of Information.) The following excerpt from the OMB guidelines should be applied in making this determination:

". . . agencies should treat requests by individuals for information pertaining to themselves which specify either the FOIA or the Privacy Act (but not both) under the procedures established pursuant to the Act specified in the request. When the request specifies, and may be processed under both the FOIA and the Privacy Act, or specifies neither Act, Privacy Act procedures should be employed. The individual should be advised, however, that the agency has elected to use Privacy Act procedures, of the existence of the general effect of the Freedom of Information Act, and the differences, if any, between the agency's procedures under the two Acts (e.g., fees, time limits, access, and appeals). The net effect of this approach should be to assure the individuals do not, as a consequence of the Privacy Act, have less access to information pertaining to themselves than they had prior to its enactment."

(2) Inform the individual whether a system of records contains a record pertaining to him or her.

(3) Permit the individual (and, at the individual's request, a person of his/her own choosing) to review the record, and have a copy made of all or any portion thereof in a form comprehensible to the individual and at a reasonable cost. (See appendix 1)

(4) Deny the request if the record sought contains information compiled in reasonable anticipation of a civil action or proceeding or if, and to the extent that, an exemption from access has been made by the FAA for that particular system of records.

b. The agency shall require the individual to furnish a written statement authorizing discussion of the individual's record in the accompanying person's presence.

c. The description of each system of records maintained by FAA and published in the Federal Register contains instructions to the public on preparing and presenting requests for access to their own records or to records of others. The public notice identifies systems of records, including content, and the office address of the system manager. Requesters have been urged to visit or write directly to the system manager, to mark the outside of their correspondence "Privacy Act," and to provide specific information to assist the FAA in processing their requests. It is anticipated, however, that some requests will be misdirected, lack the required information, or be otherwise deficient.

d. Any FAA employee receiving a request for access to a record, whether in person or by mail, will ensure prompt processing of the request, including necessary referrals if required. The Federal Register inventory of FAA and Office of Personnel Management (OPM) systems of records will be the principal tool by which requests can be directed to the proper person. A current listing of approved systems of records shall be maintained by each Privacy Act Coordinator in the region and centers and FAA Headquarters offices and services.

e. The FAA employee(s) handling requests for access shall make every possible effort to deal with requests in a timely, courteous, and helpful manner. The research and correspondence burden should be assumed by the agency to the maximum extent possible; it is the FAA's responsibility under the Act to refrain from imposing unnecessary burdens on the public.

f. One of the principal objectives of the Privacy Act is to provide individuals maximum feasible access to the information the Federal Government maintains about them. In responding to individuals' requests for records pertaining to them, FAA employees should be ever mindful of that goal. Employees are also reminded that the granting of access to the individual to whom the record pertains may not be conditioned on any requirement to state a reason or otherwise justify the need to gain access.

SECTION 2. HANDLING REQUESTS FOR RECORDS AND CORRECTIONS

2-4. MAIL REQUESTS FROM INDIVIDUALS FOR RECORDS PERTAINING TO THEMSELVES.

a. If the requested record is exempt from access, the system manager informs the individual in writing:

(1) The reason why the record is exempt, citing the DOT regulation or the Privacy Act provision for the exemption, and that

(2) The exemption may be appealed to the Assistant Administrator for Information Technology. (See paragraph 2-8)

b. If the DOT regulation does not specifically exempt a record from access, and there is no Privacy Act provision that prohibits access, the system manager proceeds with the following steps to release the record to the requesting individual. (Any decision to deny access must be concurred in by the Regional or Center Assistant Chief Counsels or Chief Counsel as appropriate.):

(1) Verifies to his/her own satisfaction the identity of the individual. If the individual cannot provide suitable identification, he/she will be required to sign a statement asserting his/her identity and attesting that he/she understands that knowingly and willfully seeking or obtaining access to records about another individual under false pretense is a misdemeanor punishable by a fine up to $5,000. If the information sought is particularly sensitive, a signed and notarized statement of identity may be required.

(2) Obtains from the individual additional information to process the request.

(3) If the record contains medical information (including psychological information furnished by a physician) and if the cognizant medical officer has determined that release of such records directly to the individual may have an adverse effect on his/her health or well being, the records should be released only through a physician designated by the individual and upon written request by such physician. Determination of such adverse effect must be made by the cognizant medical officer, with the concurrence of the General Counsel, C-1. Requests for concurrence of C-1 shall be processed through the Office of Aviation Medicine, AAM-1 and the Office of the Chief Counsel, AGC-1.

(4) If the request cannot be processed within 10 working days, acknowledges receipt of the request and informs the individual of the approximate date when access may be granted.

(5) If the record is maintained in a form readily comprehensible and appropriate for immediate retrieval and release, notifies the individual of the fee, if required, for the copying service (see Appendix 1) and transmits the copy of the record as soon as the fee, if required, is received.

(6) If the record is not readily retrievable in a form comprehensible to the individual, inform the individual of the date or approximate date on which the record will be available for review and at what cost, if any. In only very rare and exceptional circumstances should access be delayed more than 30 days. The individual should be notified of all delays in excess of 30 days.

(7) Keeps a record or log of the request for biennial reporting purposes.

2-5. IN-PERSON REQUESTS FROM INDIVIDUALS FOR RECORDS PERTAINING TO THEMSELVES.

a. If the requested record is exempt from access, the system manager informs the individual (in writing if the individual requests):

(1) The reason why the record is exempt, citing the DOT regulation or the Privacy Act provision for the exemption, and that

(2) The exemption may be appealed to the Assistant Administrator for Information Technology. (See paragraph 2-8)

b. If the DOT regulation does not specifically exempt the requested record from access, and there is no Privacy Act provision that prohibits access, the system manager:

(1) Verifies to his/her own satisfaction the identification of the individual (see paragraph 2-4b(1)).

(2) Obtains from the individual additional information to process the request.

(3) If the record contains medical information (including psychological information furnished by a physician) and if the cognizant medical officer has determined that release of such information directly to the individual may have an adverse effect on his/her health or well being, the information should be released only through a physician designated by the individual and upon written request by such physician. Determination of such adverse effect must be made by the cognizant medical officer, with the concurrence of the General Counsel, C-1. Requests for concurrence of C-1 shall be processed through the Office of Aviation Medicine and Office of the Chief Counsel.

(4) If the individual is accompanied by another person, obtains a written authorization from the individual to divulge to and/or discuss the record with or in the presence of the accompanying person.

(5) If the record is maintained in a form readily comprehensible and appropriate for immediate retrieval and release, notifies the individual of the fee, if required, for the copying service (see Appendix 1) and transmit the copy of the record as soon as the fee, if required, is received.

(6) If the request cannot be processed immediately:

(a) Informs the individual of the approximate time or date on which the record will be available for review.

(b) Reaches agreement with the individual on whether the individual will revisit the facility to review the record or if the record will be supplied in some other manner and at what cost, if any.

2-6. THIRD PARTY REQUESTS.

This paragraph applies to requests from a person, agency, or organization for individually identifiable records pertaining to others. The same procedures apply to mail and/or in-person requests.

a. The system manager:

(1) Determines if the request can be granted under one of the disclosure provisions of paragraph 2-1.

(2) Estimates time required to comply with the request. If processing the request is expected to take more than 10 working days, acknowledges receipt and informs the requester the date when final action is anticipated.

(3) Processes the request.

(4) Returns the request, if not accompanied by an appropriate signed release or if not otherwise grantable under any one of the provisions of paragraph 2-1, with a statement that such a release is required before the request can be granted.

Note: If the request is for information about a deceased individual in a Privacy Act system of records, that request should be handled as an FOIA request. The rights of a deceased individual are not protected under the Privacy Act.

(5) If system manager is below the division level, forwards the request to his or her immediate supervisor if denial is recommended unless denial is authorized by paragraph 1-6 a(2). Reasons for recommended action will accompany the forwarded request.

(6) Arranges for the filing of copies of appropriate documents pertaining to the case when the final decision has been made.

b. The system manager's immediate supervisor, if appropriate, reviews the request and the other information pertaining to the case if denial is recommended, and determines whether the denial should be upheld. The Regional or Center Assistant Chief Counsel, or Chief Counsel must be consulted prior to the final decision. When the decision has been made, the request shall be treated as an individual request and processing completed as prescribed above provided, however, that if disclosure is denied, the procedures for appeal from such denial shall be as described in paragraph 2-8 . A copy of any denial or partial denial will be forwarded to AIT-400.

2-7. CORRECTIONS TO RECORDS.

The system manager must acknowledge in writing all requests to amend a record within 10 working days of receipt of the request, and should either promptly inform the individual of the decision or indicate when a decision will be forthcoming. The individual should also be notified if any further delay occurs. A copy of the notification should be retained in a suspense file until action is completed.

a. The system manager:

(1) Determines if there is sufficient information to act on the request for amendment. If there is not, asks for additional information from the requester and includes a copy of the request in a suspense file.

(2) Reviews the record and the request to determine whether the record should be amended. This determination is based on whether the record is accurate, relevant, timely, or complete.

(3) Makes the decision to amend the record and performs the following:

(a) Amends the record or initiates the action to have the record amended.

(b) Notifies the individual in writing of the change, and attaches a copy of the amended record or the change order initiated.

(c) Notifies persons or agencies to whom the record has been disclosed that the record has been amended and indicates the substance of the amendment.

(d) Establishes such files as may be necessary for followup or reporting purposes.

NOTE: If the system manager is below the division level, the system manager will coordinate with his/her supervisor at division level or higher.

(4) If denial is recommended, prepares and forwards to the next line supervisor, if appropriate, the request from the individual, and fully detailed reasons for denying the request, and a proposed letter to the individual denying the request. See also paragraph 2-8.

(5) The system manager or supervisor at the division level or above performs the following, if after concurrence in by the appropriate legal counsel, he or she decides that the amendment should not be made:

(a) Transmits a letter of denial to the individual; and

(b) Establishes a case file, as necessary, for followup or reporting purposes.

SECTION 3. APPEALS

2-8. ADVISING REQUESTER OF RIGHTS TO APPEAL.

The following procedures shall be followed if an initial determination is made that access is not to be granted or a record is not to be amended.

a. The requester is to be given a written reason for that determination.

b. The name and title of position of each person responsible for denial of the request is to be given to the requester.

c. Advise the person who made the request that each appeal must be made in writing and must include all information relied upon by the requester. It is recommended that such request be made within 180 days of the date of the initial denial; however, exceptions to this time period will be considered in the event that a longer time is required for good reasons.

d. Advise the requester that each appeal must indicate that it is an appeal from a denial of a request made under the Privacy Act. The envelope in which the appeal is sent should be marked prominently with the words "Privacy Act." The 30–working–day time limit for responding to the appeal will not begin to run until the letter has been identified by an FAA or OPM employee as an appeal under the Privacy Act and has been received by the appropriate office.

e. When the record in question is a personnel record, advise the requester of the appropriate place and form for filing the appeal, in accordance with the applicable provisions of paragraph 4-12b(2)(d) or 4-13h(4)(c).

f. When the record in question is ***NOT*** a personnel record, advise the requester that the letter should be addressed to the Assistant Administrator for Information Technology, AIT-1, 800 Independence Avenue, SW, Washington, D. C. 20591, unless the initial determination had been made by him, in which case the letter should be addressed to the Administrator or Deputy Administrator.

2-9. INTERNAL FAA APPEALS PROCEDURES.

Appeals of initial determinations not to grant access or correct a record are to be processed as outlined in this paragraph. If the review cannot be completed within 30 working days, the Manager, IT Information Management Division, as the FAA Privacy Act Coordinator, will officially extend the period and notify the individual in writing of the extension, indicating when a decision will be forthcoming. A copy of the notification is to be retained in a suspense file until the action is completed.

a. The Assistant Administrator for Information Technology, AIT-1, is the person who will receive the appeal.

b. AIT-1 will forward the appeal to the Operational Privacy Act Coordinator, AIT-400, who shall:

(1) Maintain a log of all appeals; and

(2) Obtain the case file from the office which issued the initial denial, and obtain any other information needed by the Office of the Chief Counsel to prepare a response to the appeal.

(3) File copies of the completed determination letters.

c. The Office of the Chief Counsel, General Law Branch, AGC-110, will prepare a response using the information provided to make recommendations as to the disposition of the request for reconsideration. The response will be made for the signature of the Assistant Administrator for Information Technology, AIT-1, unless AIT-1 is a party to the appeal, in which case the Administrator or designee is the final authority. Regardless of the signature authority, all responses to appeals will be processed through the Operational Privacy Act Coordinator, in AIT-400.

d. Based on AGC's recommendations, the following actions will occur:

(1) If the recommendation is to grant access, initiate action to have access granted, and prepare a response for the signature of AIT-1 to the requester advising

him or her of the decision. Process the response through AIT-400.

(2) If the recommendation is to correct the record as requested, initiate action to correct the record, prepare a response for AIT-1 signature to the requester, attaching a copy of the corrected record or the change order initiated, and process the response to the requester through AIT-400.

(3) If the recommendation is to correct the record, the manager of that Privacy Act system will upon notification:

(a) Notify the persons or agencies to whom the old record had been disclosed that the record has been amended and indicate the substance of the change.

(b) Establish such files as may be necessary for followup or reporting purposes.

(4) If the recommendation is to affirm the initial denial not to grant access to or correct the records, the following actions will be performed by AGC-110:

(a) Prepare a letter of denial to the individual and coordinate the decision with the Office of the General Counsel, C-10, at the Department level. The letter should include:

1 A justification for refusal of the appeal,

2 The names and titles of positions of each person responsible for denial of the appeal, and .

3 A statement advising the requester that he/she may file a concise statement setting forth the reasons for disagreement with the denial of his/her appeal to correct a record; that any statement of disagreement which the individual files will be made available to anyone to whom the record is subsequently disclosed together with, at FAA's option, a brief statement by the FAA summarizing its reasons for refusing to amend the record; and that prior recipients of the disputed record will be provided a copy of any statement of disagreement to the extent that an accounting of disclosures was maintained.

4 Notification that the determination may be appealed to the district court of the United States in the district in which the complainant resides, has his or her principal place of business, or in which the records are located, or in the District of Columbia.

(b) Forward the completed action package to AIT-1 through AIT-400 for final decision and signature.

e. The Assistant Administrator for Information Technology, AIT-1, or, if applicable, the Administrator or Deputy Administrator, shall serve as the final FAA reviewing official and is empowered to take final action with regard to denial of the requested access to or correction of a record.

f. The Operational Privacy Act Coordinator will notify the appropriate organizational Privacy Act Coordinator in the office responsible for the initial denial of the action taken on the appeal.

SECTION 4. CIVIL REMEDIES

2-10. DESCRIPTION OF CIRCUMSTANCES.

a. This paragraph describes the circumstances under which an individual may seek court relief in the event that a Federal agency violates any requirement of the Privacy Act or any rule or regulation promulgated thereunder. It should be noted that an individual may have grounds for action under other provisions of law, for example:

(1) An individual may seek judicial review under other provisions of the Administrative Procedure Act.

(2) An individual may file a complaint alleging possible criminal misconduct under paragraph 2-15, Penalties.

(3) A Federal employee may file a grievance under personnel procedures.

b. The authorization for civil action by individuals is designed to ensure that an individual will have a remedy in the Federal district courts if he or she:

(1) Was unsuccessful in an attempt to have an agency amend his or her record;

(2) Was improperly denied access to his or her record or to information in a record;

(3) Was adversely affected by an agency action based upon an improperly constituted record; or

(4) Was otherwise injured by an agency action in violation of the Act.

2-11. JUDICIAL REVIEW OF AGENCY'S REFUSAL TO AMEND A RECORD.

An individual may seek judicial review of FAA's determination not to amend a record pursuant to his or her request

filed under paragraphs 2-8—2-15 under the following conditions:

a. The individual has exhausted all administrative recourse under the procedures established by FAA pursuant to paragraphs 2-8—2-15, and the agency has refused to amend the record.

b. The individual contends that FAA has not considered the request to review in a timely manner or otherwise has not acted in a manner consistent with the requirements of the Act.

2-12. JUDICIAL REVIEW OF AGENCY'S DENIAL OF ACCESS TO A RECORD.

a. Individuals may seek judicial review of FAA's determination not to grant access to records to which they consider themselves entitled, provided the individual has exhausted all administrative resources under the procedures established by FAA pursuant to paragraphs 2-8—2-15.

b. The actions giving rise to the suit may be the agency's determination to exempt a system of records from the requirements that individuals be granted access. "Since access to a file is the key to ensuring the citizen's right to accuracy, completeness, and relevancy, a denial of access affords the citizen the right to raise these issues in court. This would be the means by which a citizen could challenge any exemption from the requirements of [the Act]" (OMB Guidelines). It should be noted that particular systems of records may be exempted from the requirement of access.

c. Individuals may also contest an agency's refusal to grant access because of its interpretation of the Act or because it considers the information sought to have been compiled in reasonable anticipation of a civil action or proceeding.

d. No test of injury is required to bring action under this provision.

2-13. JUDICIAL REVIEW OF AGENCY'S FAILURE TO MAINTAIN A RECORD PROPERLY.

a. An individual may bring a civil action against the Government if an agency makes an adverse determination concerning the individual as a result of the agency's failure to maintain records about the individual that are accurate, relevant, timely, and complete.

b. An adverse determination is one resulting in the denial of employment or a right, benefit, or entitlement by the agency.

c. Damages may be assessed against the Government in the civil action if the agency's failure to maintain accurate, relevant, timely, and complete records was intentional or willful.

2-14. JUDICIAL REVIEW OF OTHER FAILURES OF THE AGENCY TO COMPLY WITH THE ACT.

In addition to the grounds specified in paragraphs 2-10 through 2-13 above, an individual may bring an action for any other alleged failure by the agency to comply with the requirements of the Act or failure to comply with any rule published by FAA to implement the Act, provided it can be shown that:

a. The action was "intentional or willful;"

b. The agency's action had an "adverse effect" upon the individual; and

c. The "adverse effect" was causally related to the agency's actions.

NOTE: Quotes are from OMB Guidelines.

SECTION 5. CRIMINAL PENALTIES

2-15. PENALTIES.

An FAA employee who is convicted of one of the following violations of the Privacy Act shall be guilty of a misdemeanor and may be subject to a fine up to $5,000.

a. **Unauthorized Disclosure.** It is a criminal violation of the Privacy Act to knowingly and willfully disclose information contained in a system of records without the prior written consent of the individual to whom it pertains, or for one of the reasons set forth in paragraph 2-1.

b. **Failure to Publish a Public Notice.** It is a criminal violation of the Privacy Act to willfully maintain a system of records without meeting the public notice requirements outlined in paragraph 7-1.

c. **Obtaining Records under False Pretenses.** It is a criminal violation of the Privacy Act to knowingly and willfully request and obtain any record concerning an individual under false pretenses.

SECTION 6. FEES

2-16. WHEN TO CHARGE FEES.

The guidance for fees is set forth in 49 CFR, subpart H, section 10.71 - 10.77. Complete guidance can be found in appendix 1 of this order. To avoid confusion, that guidance will not be repeated in this section. Please refer to the appendix.

CHAPTER 3. COLLECTION AND MAINTENANCE OF SYSTEMS OF RECORDS

3-1. GENERAL STATEMENT.

One of the key objectives of the Privacy Act is to reduce the amount of personal information collected by Federal agencies thereby reducing the risk of intentional or inadvertent, improper use of personal data. It is therefore incumbent on the FAA to review existing practices for collecting and disclosing information. The following questions should be considered by all employees requesting information and by those reviewing information previously collected:

a. How does the information relate to the purpose (in law) for which the system is maintained?

b. What are the adverse consequences, if any, of not collecting that information?

c. Could the need be met through the use of information that is not in individually identifiable form?

d. Does the item need to be collected on every individual who is the subject of a record in the system or would a sampling procedure suffice?

e. At what point will the information have satisfied the purpose for which it is collected; i.e., how long is it necessary to retain the information? Consistent with the Federal Records Act and related regulations, could part of the record be purged?

f. What are the costs/benefits of maintaining the system?

g. Is each item of information absolutely essential?

h. What security measures will be required? What will these measures cost?

NOTE: These questions are not all inclusive nor are they applicable to all systems of records, however, where applicable, they should be considered.

3-2. PROCEDURES FOR COLLECTING INFORMATION.

Information must be collected to the greatest extent practicable directly from the individual about whom the information pertains whenever such information may result in an adverse determination affecting such individual's rights, benefits, or privileges under a Federal program. It should be noted also, that disclosure of a Social Security number is voluntary on the part of the individual unless such disclosure is required by Federal statute or regulation adopted prior to January 1, 1975, to verify the identity of an individual. Employees are, for example, required to give their social security numbers for payroll and related purposes. There is no set rule for Privacy Act statements. However, each form which is used to collect privacy information shall contain all the elements described in the general rules which follow.

a. **General Rules or Instructions For Collecting Information.** Each individual asked to supply information about himself/herself to FAA must be advised of the following on the form used to collect information, or on a separate form that can be retained by the individual:

(1) The authority for making the request and whether disclosure is mandatory or voluntary.

(2) The principal purpose(s) for which the information is intended to be used.

(3) The routine uses which may be made of the information.

(4) The effects on the individual of not providing all or any part of the requested information.

b. **Rules for Requesting Social Security Numbers (SSNs).**

(1) No agency employee in the course of his or her official duties shall REQUIRE any person to disclose his or her SSN unless such disclosure is specifically required by Federal statute or by a Federal regulation effective prior to January 1, 1975. When such disclosure is so required, the person from whom the disclosure is sought shall be informed:

(a) That submission of the social security number is mandatory. The Federal statutory authority or pre-January 1, 1975 regulation under which submission of the social security number is required shall be identified.

(b) Of the uses that will be made of the social security number.

(2) Whenever the submission of a social security number is voluntary, any agency employee requesting an SSN from an individual shall inform such person:

(a) That the submission of an SSN is not required by law and an individual's refusal to furnish an SSN will not result in the denial of any right, benefit, or privilege provided by law.

(b) That if the individual refuses to supply an SSN, a substitute number or other identifier will be assigned in those records where such an identifier is needed.

(c) That the SSN, if supplied, is used by the FAA to associate the current information relating to the individual with other information about the same individual FAA may have in its files from previous transactions.

(d) That the SSN is solicited to assist in performing the agency's functions under the Federal Aviation Act of 1958, as amended (or other authority, if applicable).

(3) When a form is used to collect an SSN from an individual, the disclosure of which is required by Federal statute or pre-January 1, 1975 regulation, the information required in paragraphs 3-2b(1)(a) and (b) must be printed on the form or on a flyer attached to the form.

(4) When a form is used to obtain the voluntary disclosure of an SSN from an individual, the information required in paragraphs 3-2b(2)(a), (b), (c), and (d) must be printed on the form or on a flyer attached to the form.

(5) Offices that administer programs using contractors or agents, who are not FAA employees, who request or require disclosure of SSNs from individuals must notify such agents of the provisions of this order and require them to comply.

c. **Third Party Sources.** Practical considerations may dictate that a third party source, including systems of records maintained by other agencies, be used as a source of information. Prior to contacting a third party source, consider the following points:

(1) The nature of the requirement.

(2) The cost of collecting the information directly from the individual as compared with a third party.

(3) The risk that the particular elements of information proposed to be collected from third parties, if inaccurate, could result in an improper and adverse determination.

(4) The need to ensure the accuracy of information supplied by a third party source.

(5) Provisions for verifying the accuracy of third party information prior to making a determination regarding the subject individual based on that information. In verifying the accuracy of third party information, all requirements of the Privacy Act must be complied with.

NOTE: Requests for personal information from another agency concerning employees are also subject to these considerations. The act of informing an individual of the possible uses that may be made of the information at the time he or she is supplying it does not satisfy the Act's requirement for prior consent unless the disclosure is excepted from that requirement. (See paragraph 2-1, Conditions of Disclosure)

3-3. MAINTENANCE OF RECORDS.

a. FAA shall maintain all records which are used in making determinations about an individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual in the determination process.

b. Prior to disseminating any record about an individual to any person or to another agency, FAA shall make reasonable efforts to ensure that such records are accurate, complete, timely, and relevant for agency purposes.

c. FAA shall not maintain any records describing how an individual exercises rights guaranteed under the First Amendment unless expressly authorized by statute or by the individual to whom the record pertains. This provision includes, but is not limited to, religious and political beliefs, freedom of speech and of the press, and freedom of assembly and to petition.

3-4. RECORDS MADE AVAILABLE UNDER COMPULSORY LEGAL PROCESS.

FAA shall make reasonable efforts to serve notice on an individual when any record on such individual is made available to any person under compulsory legal process when such process becomes a matter of public record. The person disclosing the information must send a notice to the individual's last known address, and retain adequate documentation of such mailing. There is no obligation under the law to ensure delivery of notification.

3-5. RECORDS INVOLVED IN COMPUTERIZED MATCHING PROGRAMS.

a. A matching program, which at its simplest, is defined as the comparison of records using a computer. The records must themselves exist in automated form in order to perform the match. Manual comparisons of printouts of two automated data bases are not included within this definition. The Computer Matching Act covers two kinds of matching programs: (1) matches involving Federal benefits programs and, (2) matches using records from Federal personnel or payroll systems of records.

b. Before one agency can be involved in a Privacy Act matching program with another agency, certain administrative procedures and documentation containing justification for approval must be accomplished. The agency receiving the computerized records to use in a match with its own computerized records must prepare a matching agreement with the source agency. This agreement and subsequent justification for approval would need to contain the following: the purpose and legal authority for the match, the justification and expected results of the match, a description of the records being used in the match, notification procedures, verification procedures; disposition of matched items, security procedures, records usage, duplication and redisclosure restrictions, records accuracy assessments, and Comptroller General access.

c. All computer matches, whether or not they are believed to be covered under the Privacy Act, are to be brought before the Departmental Data Integrity Board. In order to do that, the program office must contact the FAA

Data Integrity Review Committee through the Assistant Administrator for Information Technology, AIT-1, as the chair, and request a review of the proposed matching program.

d. Since the OMB guidelines for computer matches under the Privacy Act are quite long and involved, and all matters whether or not covered under the Privacy are brought before the departmental Data Integrity Board, the actual guidelines explaining what constitutes a Privacy Act matching program and all the procedures for review will not be published in this order. Any organization wanting a copy of the guidelines can contact the FAA Operational Privacy Act Coordinator, AIT-400.

3-6. RECORDS SAFEGUARDS.

Chapter 5, Safeguarding Privacy Act Records, provides basic FAA administrative, technical, and physical security policies. These are intended to ensure the security and confidentiality of manual and automated records and to protect them against anticipated threats to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

3-7. TRANSFER OF RECORDS.

a. **Federal Records Center.** Each record transferred shall, for purposes of the Privacy Act, be considered the property of FAA. The National Archives and Records Center, NARA, will not disclose any information except to personnel authorized to retrieve the records. The procedures established in the current version of Order 1350.14, Records Management, should be followed with regard to access to records stored in Federal Records Centers.

b. **Archival Records.** Records normally are transferred to the National Archives from a Federal Records Center. Each agency record pertaining to an individual which is transferred to the National Archives after September 27, 1975, as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, shall be considered the property of the National Archives and not be subject to many of the provisions of the Act; however, such records must be included in the notice of systems of records published in the Federal Register. Each office must examine its records of transfer to ensure compliance with this provision of the Act. Offices should not retain records simply to facilitate retrieval as this would defeat the purpose of centralized storage of Federal records and would be inconsistent with one of the purposes of the Privacy Act; i.e., non disruption of existing Federal programs and procedures.

c. **Transfer of Records other than to Federal Records Centers.** Procedures established in the current version of Order 1350.14, Records Management, chapter 7, should be followed. This transfer of records constitutes a disclosure and an accounting is required. (See paragraph 3-8)

3-8. ACCOUNTING OF CERTAIN DISCLOSURES.

The Act requires that agencies account for disclosure of records.

a. **Exclusions from Accounting.** The only disclosures that do not have to be accounted for are:

(1) The release of information to the individual to whom it pertains. However, if the individual cites the Privacy Act in his/her request, a record must be kept for the Privacy Act Biennial Report.

(2) Disclosures to agency officials and employees who have a need for the record in the performance of their duties.

(3) Disclosures required under the Freedom of Information Act (FOIA). This is interpreted to mean FAA does not have to account for disclosures required under FOIA. However, requests for information of a personal nature that may be withheld from the public but are disclosed must be accounted for by the agency. Order 1200.23, Public Availability of Information, lists the records that may be withheld from disclosures to the public.

b. **Disclosure Accounting Requirements.**

(1) Managers of systems of records shall:

(a) Keep an accurate accounting of:

1 The date, nature, and purpose of each disclosure of a record to any person outside DOT or to another agency.

2 The name and address of the person or agency to whom the disclosure was made.

(b) Retain the accounting for at least five years or the life of the record whichever is longer, after the disclosure for which the accounting is made. Refer to the current version of Order 1350.15, Records Organization, Transfer, and Destruction Standards.

(c) Make the accounting available to the individual named in the record at his/her request, except for those records exempted from this requirement of the Act and those records released to another agency or to a Governmental instrumentality for an authorized civil or criminal law enforcement activity under subsection (b)(7) of the Act.

(d) Inform any person or other agency previously given Privacy Act data about any correction or notation of dispute made by FAA as a result of an individual's request to have his/her record amended.

(2) No standardized form or format will be prescribed for this purpose. However, an existing form, FAA Form 1300-11, History, NSN 0052-00-8 08-9000, Unit of Issue: Sheet, could be used depending upon the nature of the system. Other system managers may find plain, white paper satisfactory for logging information that meets the disclosure accounting requirement. For automated systems, an automated accounting system can be developed. Systems managers may amplify this paragraph if additional, specialized data are required, and report their recommendations to the FAA Privacy Act Coordinator.

c. Procedures for Disclosure Accounting.

(1) Requests from an individual for an accounting of disclosures from his/her records shall also be accounted for.

(2) Disclosure records must be retained at least five years after disclosure or the life of that particular record, whichever is longer.

(3) Mass transfers of records outside FAA, such as transfers to disbursing offices for issuing payroll checks, are not to be recorded on an individual basis. However, the information must be retrievable on an individual basis since an individual listed in a system of records can request an accounting of disclosures of personal data pertaining to him/her from these records. The information provided the individual must be in a format that is understandable by the average individual. It is vitally important that mass transfers of records be listed as a routine use of that particular system of records in the notice to be published in the Federal Register. Therefore, prior written consent of the individual would not be required and the concerned individual must request an accounting of disclosures in order to know what information of a personal data was actually disclosed.

(4) A system of accounting for disclosures is not considered a system of records for purposes of the Privacy Act, and does not have to be included in the published list of systems of records.

d. Maintaining Records of Disclosures and Related Activities. Each location maintaining records of any published system of records shall maintain a record of all disclosures and related activities.

CHAPTER 4. PERSONNEL RECORDS

SECTION 1. GENERAL

4-1. COVERAGE.

This chapter provides instructions and guidance concerning the Privacy Act as it relates to personnel records (defined in paragraph 1-7m).

4-2. CHANGES.

Changes to this chapter, paragraph 1-7m, or to the systems notices cited in paragraph 1-7m, must be coordinated with the Director of Personnel.

4-3. DEFINITIONS.

The terms listed here carry special definitions for the purposes of this chapter. Other terms used are defined in paragraph 1-7.

a. **Employee** means a current or former FAA employee.

b. **Applicant** is an individual who has applied for FAA employment.

c. **Personnel Records System Managers** (see paragraph 1-7t) are the Personnel Management Information Systems Managers in Washington Headquarters, the regions, and the centers.

(1) The human resource organization manager, or subordinate designated by him/her, is the system manager for personnel records maintained by the organization.

(2) Supervisors of offices which maintain authorized personnel records (see paragraph 4-28) concerning their employees are system managers for those records.

(3) Superintendents of the FAA Academy and the FAA Center for Management Development are systems managers for the training records maintained at their respective locations.

(4) System notices will designate the system manager for any personnel records not covered by 4-3c(1), (2), and (3) above.

d. A Personnel Privacy Act Officer is the person who shall be designated by each region and center human resource organization manager to carry out the responsibilities described in paragraph 4-4.

4-4. RESPONSIBILITIES OF THE PERSONNEL PRIVACY ACT OFFICER.

a. Assisting the human resource organization manager in discharging his/her personnel management responsibilities under the Privacy Act and this order.

b. Ensuring that human resource organization employees and FAA supervisors are made aware of their responsibilities regarding personnel records under the Act.

c. Serving as the human resources organization communication channel and providing advice and assistance regarding the personnel implications of the Act.

d. Ensuring that personnel orientation programs include a general discussion of individual employee responsibilities under the Privacy Act.

e. Cooperating with the jurisdiction's Privacy Act Coordinator.

g. Referring unresolved problems to the jurisdiction's Privacy Act Coordinator. If Headquarters advice is needed the Privacy Act Coordinator and the Personnel Privacy Act Officer will determine whether a problem shall be referred to the FAA Operational Privacy Act Coordinator. Questions involving the interpretation of the Act and implementing regulations should be referred to the local FAA Assistant Chief Counsel.

4-5. OFFICE OF PERSONNEL MANAGEMENT (OPM) REGULATIONS.

Regulations regarding implementation of the Privacy Act are found in 5 CFR, Parts 293 and 297, and are available in all FAA personnel offices. Provisions of these regulations have been amplified and incorporated into this chapter whenever possible. However, in a few instances, it is necessary to cite these regulations directly because pertinent material is either too lengthy or infrequently used to justify inclusion in this chapter. Supervisors needing assistance regarding the regulations should contact their human resource organization. Any unresolved questions should be referred in accordance with paragraph 4-4g.

4-6. OPM/GOVT SYSTEMS NOTICES are published in the Federal Register. Copies are maintained by Privacy Act Coordinators and Personnel Privacy Act Officers.

SECTION 2. DISCLOSURE OF PERSONNEL RECORDS

4-7. CONDITIONS OF DISCLOSURE.

The agency's policy on disclosure of personnel records is stated in paragraph 1-9a. Prior written consent, if obtained, must be specific, not open-ended; i.e., the employee's or applicant's consent must state the general purpose for and names and types of recipients to whom disclosure(s) may be made. Paragraphs 2-1 and 6-5 list the conditions when disclosures of personnel records may be made WITHOUT prior written consent. Paragraph 2-6 describes procedures for processing requests from third parties.

a. One of the conditions for which an employee's or applicant's prior written consent is not required is disclosure of a record to a member of the public to whom FAA is required to disclose such information under the Freedom of Information Act. The following information contained in personnel records must be disclosed under the Freedom of Information Act, upon request: employee's name, present and past Federal position titles, grades, salaries, and duty stations (which include room numbers, shop designations, or other identifying information regarding buildings or places of employment). This information will not be disclosed when disclosure would constitute a clearly unwarranted invasion of personal privacy because the manner in which the request is phrased would call for a response that would reveal more about the employees on whom information is sought than the five above described items, or when the information is otherwise protected from disclosure under an exemption of the Freedom of Information Act. (See Order 1200.23, Public Availability of Information, paragraph 5, for a discussion of these exemptions.)

b. Notwithstanding the above provision, disclosures may be made without prior written consent of the employee concerned if the disclosure meets any condition listed in paragraphs 2-1 and 6-5. For example, disclosures may be made for a routine use which has been established and described in the public notice required by the Act to be published in the Federal Register. Examples of utilization of this routine use provision follow:

(1) A prospective employer (outside of DOT) or lending institution contacts an FAA personnel office requesting information contained in personnel records beyond that required to be disclosed under the Freedom of Information Act and the request is not accompanied by the employee's prior written consent. The personnel office, AS AN ALTERNATIVE TO OBTAINING OR ASKING THE REQUESTER TO OBTAIN WRITTEN CONSENT, may disclose the information under an appropriate routine use described in the System Notice. For example, OPM/GOVT 1, which includes the Official Personnel Folder, includes as a routine use disclosure "...to prospective employers or other organizations, at the request of the individual." In this case, the personnel office may disclose the information AT THE EMPLOYEE's REQUEST WHICH NEED NOT BE IN WRITING.

(2) It is expected in most cases, that the personnel office will obtain prior written consent for disclosures of personnel records. However, in an unusual situation such as when the employee wishes that an expeditious response be made to the inquiry and, for example, is located at a work site remote from the personnel office, he/she may orally request that the disclosure be made. If that request is consistent with a published routine use, the personnel office should make a record that the disclosure was made at the request of the employee and the specific items of information requested to be disclosed by the employee.

c. Disclosures of personnel records may also be made without the employee's prior written consent to:

(1) A survivor of a deceased employee, or annuitant, or an individual authorized to act in his/her behalf.

(2) A parent or legal guardian of an employee under 5 U.S.C., section 552a(h).

d. The OPM regulations, 5 CFR Part 297, describe specific procedures applicable to disclosure of and granting access to certain personnel records, including medical and investigative records, examination and related material, appeals files, and Part 713 discrimination complaint files. These procedures are to be followed (where applicable) in making disclosures from or granting access to those personnel records. See also paragraphs 2-4b(3) and 2-5 b(3) for additional provisions regarding medical records only.

e. Special procedures regarding disclosures of certain personnel records in response to CONGRESSIONAL INQUIRIES ONLY are described in paragraph 4-24.

4-8. ACCOUNTING FOR CERTAIN DISCLOSURES OF PERSONNEL RECORDS is required (see paragraph 3-8). However, some OPM/GOVT personnel records are exempted from the requirement of making the accounting of disclosures available to the employee or applicant. These records are discussed in Part 297 of the OPM regulations.

4-9. DISCLOSURES WITHIN FAA.

When personnel records are disclosed from one organizational unit to another (such as transmission of an Official Personnel Folder from a personnel office to a supervisor or another personnel office for review) the receiving unit or individual is also responsible under the Act for maintaining them, including any further dissemination.

SECTION 3. ACCESS TO AND CORRECTION OF PERSONNEL RECORDS AND PRIVACY ACT INQUIRIES

4-10. GENERAL.

The procedures described in the following paragraphs, 4-11, 4-12, and 4-13, necessarily include provisions mandated by the OPM regulations relating to access and correction of personnel records which are in some cases more rigorous than the FAA requirements described in chapter 2, sections 2 and 3 (which relate to all other FAA systems of records). In order to ensure clarity and consistent application of both FAA and OPM provisions relating to access to and correction of personnel records, they have been merged in this section. This minimizes but does not eliminate cross-referencing to other parts of this order.

4-11. GRANT OF ACCESS.

An employee or applicant shall be granted access to personnel records pertaining to him/her upon request. When a mail or in-person request for access has been received, the system manager or an individual designated by the system manager shall:

a. Determine whether the request should be handled under Freedom of Information Act (FOIA) or Privacy Act procedures. (See paragraph 2-3a(1))

b. Inform the requester whether a system of records pertains to her/him and reserve the right to require positive identification if the requester is not known to the system manager.

c. NOTIFY the requester of the following within 10 workdays:

(1) The method of access to the personnel records which may include, depending on the circumstances of a given situation:

(a) Inspection, in person, in the office specified by the system manager, during the hours specified.

(b) Transfer of the personnel records to another FAA office, an OPM office, or other Federal facility more convenient to the requester, but only if the system manager determines that a suitable facility is available, that access can be properly supervised at the facility, and that transmittal of the records to that facility will not unduly interfere with the operations of OPM or FAA or involve unreasonable costs in terms of both money and personnel.

(c) Copies may be mailed at the request of the requester, when appropriate, and subject to the payment of fees as described in paragraph 4-25.

(2) The place at which the personnel record may be inspected.

(3) The earliest date on which it may be inspected. In no event shall the estimated date be later than 30 calendar days from the date of notification.

(4) The period of time the personnel records will remain available for inspection.

(5) The estimated date by which a copy of the record could be mailed (the 30-day time limit described in paragraph 4-11c(3) applies) and an estimate of fees when appropriate and pursuant to paragraph 4-25.

(6) The fact that, if he or she wishes, the requester may be accompanied by another individual during personal inspection and review.

(7) Any additional requirements needed to grant access to a specified personnel record.

d. Observe the special procedures applicable to granting access to certain personnel records which are described in paragraph 4-7d.

e. Supply such other information and assistance at the time of access as to make the personnel record intelligible to the requester.

f. Reserve the right (when appropriate) to provide access to copies and abstracts of original records. This election would be appropriate, for example, when the record is in an automated data medium such as tape or disk, when the record contains information on other individuals, or when deletion of information is permissible under exemptions described in paragraph 4-12. In no event shall original personnel records of the OPM or the FAA be made available to the individual except under the immediate supervision of the system manager or his/her designee. Section 2701 of Title 18 of the United States Code makes it a crime to conceal, mutilate, obliterate, or destroy any record

filed in a public office, or attempt to do any of the foregoing.

g. Observe the right of any employee or applicant who requests access to a personnel record pertaining to him or her to be accompanied by another individual of his or her choice. "Accompanied" includes discussion of the record in the presence of the other individual. The person to whom the record pertains shall authorize the presence of the other individual in writing and shall include the name of the other individual, a specific description of the record to which access is sought, the date, and the signature of the individual to whom the record pertains. The other individual shall sign the authorization in the presence of the system manager or his/her designee. An employee or applicant shall not be required to state a reason or otherwise justify his or her decision to be accompanied by another individual during personal access to a record.

h. Permit the employee or applicant to have a copy of all or any portion of a personnel record pertaining to him/her, if requested. (See paragraph 4-25 regarding fees)

i. Ensure that the provisions of paragraph 2-3d, e, and f are also complied with.

j. Deny access, when applicable. (See paragraph 4-12)

k. Annotate such internal records as may be necessary for accounting of disclosures. (See paragraphs 3-8 and 4-8)

4-12. DENIAL OF ACCESS.

a. Grounds. Access by an employee or applicant to personnel records pertaining to him/her shall be denied ONLY upon a determination by the system manager or designee that one or more of the following grounds exist:

(1) For Government-wide personnel records

(a) A personnel record is subject to an exemption under Part 297 of the OPM regulations.

(b) The provisions of Part 297 of the OPM regulations pertaining to medical records apply.

(c) The personnel record is information compiled in reasonable anticipation of a civil action or proceeding.

(d) The requester refuses to provide information necessary to process the request for access.

(2) For FAA-wide personnel records

(a) The provisions of Part 297 of the OPM regulations or paragraphs 2-4b(3) or 2-5 b(3) pertaining to medical records apply.

(b) The personnel record is information compiled in reasonable anticipation of a civil action or proceeding.

(c) The requester refuses to provide information necessary to process the request for access.

b. Procedure. If access is to be denied, the system manager or designee shall:

(1) Gain concurrence from the Regional or Center Assistant Chief Counsel, or the Chief Counsel as appropriate.

(2) Provide a written notice of denial of access to the requester which shall include the following information:

(a) The system manager's or designee's name and title or position.

(b) The date of denial.

(c) The reasons for the denial including citation to appropriate sections of the Privacy Act and OPM regulations.

(d) The opportunities for appeal which depend upon the following:

1 If access to a record in a Government-wide System of Records is denied, the appeal must be filed with the Assistant Director for Workforce Information, Personnel Systems and Oversight Group, Associate Director for Agency Relations, U.S. Office of Personnel Management, 1900 E Street, N. W., Washington, D. C. 10415.

NOTE: If the denial is made under paragraph 4-12a(1)(a), the appeal must be in the form of a petition for repeal or amendment of the rule establishing the exemption. (See Part 297 of the OPM Regulations)

2 If access to a record in an FAA System of Records is denied, the appeal must be filed with the Assistant Administrator for Information Technology, AIT-1, Federal Aviation Administration, 800 Independence Avenue, SW, Washington, D. C. 20591.

4-13. REQUESTS FOR AMENDMENT OF OR CORRECTION TO PERSONNEL RECORDS.

a. An employee or applicant may submit a request for correction to or amendment of personnel records pertaining to him/her to the OPM or to the FAA. The request should be made either in person or by mail to the system manager or his/her designee indicated in the notice of systems of records. (The remainder of this paragraph deals with requests received by FAA).

b. The processing of requests submitted by mail will be facilitated if the words "PRIVACY ACT REQUEST"

appear in capital letters on the face of the envelope and in the letter of inquiry.

c. THE PROVISIONS FOR AMENDING PERSONNEL RECORDS ARE NOT INTENDED TO PERMIT ALTERATION OF EVIDENCE OR DECISIONS REACHED THROUGH ESTABLISHED GRIEVANCES AND APPEAL SYSTEMS, JUDICIAL, OR QUASI-LEGISLATIVE PROCEEDINGS. ANY CHANGES IN SUCH RECORDS SHOULD BE MADE ONLY THROUGH THE ESTABLISHED PROCEDURES CONSISTENT WITH THE ADVERSARY PROCESS. However, the individual has the right to challenge the fact that the evidence or decision has been inaccurately recorded in his/her records.

d. Any request which is not addressed as specified in paragraph 4-13a or which is not marked as specified in paragraph 4-13b will be so addressed or marked by FAA personnel and forwarded immediately to the responsible system manager. A request not properly addressed by the individual will not be deemed to have been "received" for purposes of measuring time periods for response until the responsible system manager receives it. In each instance when a request so forwarded is received, the system manager or his/her designee shall notify the individual that his or her request was improperly addressed and the date when the request was received at the proper address.

e. Since request for correction or amendment normally follows a request for access, the individual's identity should be established by his or her signature on the original request. In the event a request for correction or amendment is not preceded by a request for access, the procedures established for verification of identity in paragraph 4-11b should be utilized.

f. A request for correction or amendment should include the following:

(1) The specific identification of the record sought to be corrected or amended (for example, description, title, date, paragraph, sentence, line, and words).

(2) The specific wording to be deleted, if any.

(3) The specific wording to be inserted or added, if any, and the exact place at which it is to be inserted or added.

(4) A statement of the basis for the requested correction or amendment, with all available supporting documents and materials which substantiate the statement.

g. Not later than 10 workdays after receipt of a request to correct or amend a record, the system manager or his/her designee shall send an acknowledgment providing an estimate of time within which action will be taken on the request. If a response cannot be made within 10 workdays due to unusual circumstances, the system manager shall send an acknowledgment during that period providing information on the status of the request and asking for such further information as may be necessary to process the request. (Unusual circumstances shall include circumstances where a search for and collection of requested records from storage, field facilities, or other establishments are required, cases where a voluminous amount of data is involved, or instances where information on other individuals must be separated or deleted from the particular record.) No acknowledgment will be sent if the request can be reviewed, processed, and the individual notified of the results of review (either compliance or denial) within 10 workdays. Requests filed in writing will be acknowledged in writing. A copy of the acknowledgment will be retained in a suspense file until action is completed.

h. After acknowledging receipt of a request and receiving such additional information as might have been requested, the system manager or his/her designee shall review paragraph 4-13k and l and EITHER:

(1) IF IN AGREEMENT with the request:

(a) make the requested correction or amendment and advise the requester in writing of such action within 30 calendar days, providing either a free copy of the corrected or amended portion of the record or a statement as to the means whereby the correction or amendment was effected in cases where a copy cannot be provided (for example, erasure of information from a record maintained only in an electronic data bank).

(b) Notify all persons or agencies to which the corrected or amended portion of the personnel record had been disclosed prior to its correction or amendment if an accounting of such disclosure(s) required by the Privacy Act was made. (This notification requirement does NOT apply to disclosures made pursuant to paragraphs 2-1a-b.)

(c) Establish a case file for followup or reporting purposes.

(2) IF NOT IN AGREEMENT with the requested correction or amendment, and if the system manager is below the division level, the system manager shall prepare and forward within 10 workdays to his/her immediate supervisor:

(a) The request for correction or amendment.

(b) A recommendation and fully detailed reason(s) for denying the request.

(c) A proposed letter to the requester denying the request in accordance with paragraph 2-8 and advising the requester as follows:

1 If the denial of correction or amendment is for a record contained in a GOVERNMENT-WIDE System of Records, the appeal must be filed with the Assistant Director for Workforce Information, Personnel Systems and Oversight Group, U.S. Office of Personnel Management, 1900 E Street, NW, Washington, D. C. 20415.

2 If the denial of correction or amendment is for a record contained in an FAA System of Records, the appeal must be filed with the Assistant Administrator, Office of Information Technology, AIT-1, Federal Aviation Administration, 800 Independence Avenue, SW., Washington, DC 20591.

i. The system manager or immediate supervisor of the system manager, if appropriate, within 20 workdays:

(1) Reviews the information provided by the system manager and obtains other information pertaining to the case as required, including advice from FAA counsel.

(2) If he or she disagrees with the system manager's recommendation for denial:

(a) Directs that the change be made.

(b) Follows the procedure described in paragraph 4-12h(1).

(c) Follows the procedure described in paragraph 4-12h(2).

(3) If he or she decides that the amendment or correction should not be made:

(a) Gains concurrence from Regional or Center Assistant Chief Counsels or Chief Counsel as appropriate.

j. If the system manager (designee) cannot take the appropriate actions described in paragraphs 4-13h(1), 4-13i(2)(a) and (b), or 4-13i(3)(b) so that the employee or applicant is advised of the determination within 30 workdays, he/she shall be advised in writing of the reasons for the delay and the estimated date by which a determination will be made.

k. The following criteria are examples of those that will be considered by the system manager (designee) in reviewing a request for correction or amendment:

(1) The sufficiency of the evidence submitted.

(2) The factual accuracy of the information.

(3) The relevance and necessity of the information in terms of the purpose for which it was collected.

(4) The timeliness and currency of the information in terms of the purpose for which it was collected.

(5) The completeness of the information in terms of the purpose for which it was collected.

(6) The degree of possibility that denial of the request could unfairly result in a determination adverse to the employee or applicant.

(7) The character of the record sought to be corrected or amended.

(8) The propriety and feasibility of complying with specific means of correction or amendment requested by the employee or applicant.

NOTE: FAA will not make an effort to gather evidence for the individual but does reserve the right to verify the evidence submitted.

l. Correction or amendment of a record will be denied upon a determination by the system manager that:

(1) The information submitted is not accurate or relevant.

(2) The correction or amendment would violate an enacted statute or regulation.

(3) The personnel record is subject to an exemption under Part 297 of the OPM regulations (applies ONLY to Government-wide personnel records).

(4) The employee or applicant refuses to provide information which is necessary to process the request to correct or amend the record.

(5) If a request is partially granted and partially denied, the system manager shall follow the appropriate procedures of this order as to the records within the grant and the records within the denial.

4-14. FAA INITIATED AMENDMENT OR CORRECTION OF PERSONNEL RECORDS.

When the agency detects erroneous data in personnel records or a third party source provides corrected information, FAA will correct the record and provide all recipients of such record with the corrected information to the extent that it is relevant to the recipient's uses and deemed feasible to do so.

4-15. PRIVACY ACT INQUIRIES.

Any person may inquire for general information regarding the Act and implementing DOT and OPM regulations or request that FAA or OPM determine whether it has, in a given system of personnel records, a record which pertains to the individual. Part 297 of the OPM regulations provides procedures for handling such inquiries which shall be followed by human resource organization managers.

SECTION 4. COLLECTION AND MAINTENANCE OF PERSONNEL RECORDS

4-16. WRITTEN EXPLANATIONS described in paragraphs 3-2a and b shall be attached to or distributed with all personnel and training forms when required. Headquarters elements have developed and distributed supplements for NATIONALLY used OPM, FAA, or other forms. (Any questions regarding whether a nationally used personnel and training form is properly supplemented should be directed to the jurisdiction's Personnel Privacy Act Officer and surfaced to Washington Headquarters if necessary as described in paragraph 4-4g.) Each human resource organization is similarly responsible for supplementing LOCAL personnel and training forms.

4-17. STANDARDS OF ACCURACY FOR PERSONNEL RECORDS.

In order to minimize the risk that FAA will make an unwarranted adverse personnel determination or disseminate inaccurate information about an employee or applicant, all personnel records which are used in making any such determination shall be maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness. Criteria for accuracy in these records are:

a. The factual accuracy of the information.

b. The sufficiency of the information to make a fair and equitable determination.

c. The relevance and necessity of the information in terms of the purpose for which it was collected.

d. The timeliness and currency of the information in light of the purpose for which it was collected.

e. The completeness of the information in terms of the purpose for which it was collected.

f. The degree of possibility that the information could unfairly result in an adverse determination.

4-18. ANNUAL REVIEW ANNOUNCEMENT.

Human resource organization managers shall announce, by a notice to all current employees in their jurisdiction at least annually that, at the employee's request, he or she will be provided with an opportunity to review automated and manual personnel records that are maintained concerning the employee and that have the potential of being used in making a determination about the employee or being disclosed under routine uses outside DOT. (Procedures applicable to access to, correction of, or amendment of personnel records are described in section 3 of this chapter.)

4-19. SAFEGUARDING PERSONNEL RECORDS.

Personnel records must be safeguarded in accordance with the requirements of chapter 5. So as to ensure proper and continuing implementation of the appropriate security guidelines, each human resource organization manager shall designate a Personnel Records Security Officer (who may or may not be the Personnel Privacy Act Officer designated in accordance with paragraph 4-3e). The security officer shall assist the human resource organization manager in discharging his/her responsibilities for the security of personnel records as described in chapter 5.

SECTION 5. MISCELLANEOUS PROVISIONS

4-20. SPECIFIC PERSONNEL RECORDS.

a. **Suitability Files.** If separate personnel records containing suitability information, such as reference checks and debt complaints, are kept on individual employees, a system notice must be published. If the information is filed on the left side of the Official Personnel Folder, OPM/GOVT systems notices suffice.

b. **Merit Promotion Plan (MPP) Records.** These records which the OPM requires to be maintained are generally filed by announcement number, and the information is not retrieved by name of employee or applicant or by personal identifying number. Under these circumstances, the records are not covered by the Privacy Act. Information maintained in individual Official Personnel Folders is covered by OPM system notices. If MPP records are maintained in any other manner in which they are retrieved by name or number (such as skills files) they must be published as a system of records.

c. **Applications for Employment (e.g., Standard Form SF-171).** The OPM systems notices cover SF-171s if they are maintained in an Applicant Supply File as defined in 5 C.F.R., chapter 333. Also covered are applications which are received for a specific vacancy and returned to the applicant. SF-171s shall be maintained in an Applicant Supply File or returned to the applicant unless a different procedure is specifically authorized by the Administrator.

d. **Grievance, Arbitration, and Unfair Labor Practice/Charge Complaint Files.**

(1) Those grievance files which OPM requires agencies to keep are covered by OPM system notices.

(2) Grievance and arbitration files maintained under a negotiated agreement with a union and records on unfair labor practice charges/complaints are not covered by OPM systems notices. If such records are retrieved by employee name or number, they must be covered by a system notice. If filed by subject matter, agreement involved, third party case, or by specific provision of Executive Order 11491, and information is not retrieved by employee name or number, the records are not subject to the Privacy Act.

e. Medical Records. The OPM system notices cover medical data required by OPM. However, medical data contained in health unit records which are subject to the requirements of the Privacy Act are covered by an FAA published system notice. Alcohol and drug records subject to the Act and referenced to in 5 C.F.R., chapter 792 are covered by an OPM system notice.

4-21. CONFIDENTIAL EMPLOYMENT INQUIRIES (VOUCHERS).

a. Employees/applicants who are the subject of vouchers completed prior to September 27, 1975, may have access to those vouchers provided that the identity of the person who completed the voucher is not revealed. In clear-cut cases, this can be accomplished by removing the name of the respondent and any other material that would reveal his/her identity. "Other material" could include parts or all of Sections 1, 2, and 10 of the form. It is less likely that the respondent's identity would be revealed by granting access to parts 3 through 9. In rare cases when it is impossible to protect the identity of the respondent by excising information, the entire voucher may be withheld. (See paragraph 4-12a(l))

b. Vouchers completed on and after September 27, 1975, are handled in the same manner except that the IDENTITY of the source of the information must ALSO be revealed to the subject upon request unless an express guarantee was made to the source that his or her identity would not be revealed.

c. When a pledge of confidentiality is requested, personnel offices must take reasonable precautions to protect the source's IDENTITY ONLY under the excising procedure described above. When the pledge of confidentiality is not requested, the subject may have access to the entire voucher.

4-22. REFERENCE INQUIRIES RECEIVED.

Supervisors or other FAA employees may receive employment or reference inquiries from prospective employers of their subordinates or associates. These inquiries often request the respondent to provide his/her subjective appraisal of the applicant. These appraisals may be given without restriction if the respondent relies on his/her personal knowledge of the applicant or uncirculated personal notes only. If the respondent relies on information contained in personnel records, disclosures may be made only in accordance with the provisions of paragraph 4-7. Of course, respondents are free to request a pledge of confidentiality as to their identity in any case.

4-23. PRIVACY ACT STATEMENT FOR MPP ANNOUNCEMENTS.

DOT Form 3330.6, Promotional and Career Opportunities, includes an overprinted Privacy Act statement (see paragraph 4-16) which shall also be included in any local MPP announcements which are issued by human resource organizations on other forms.

4-24. RESPONDING TO CONGRESSIONAL INQUIRIES.

OPM/GOVT systems notices list a routine use of those systems of records as follows:

"To provide information to a congressional office from the record of an individual in response to an inquiry from a congressional office made at the request of that individual."

The application of this published routine use when disclosure of information in those systems of records TO A CONGRESSIONAL OFFICE is anticipated, is discussed below.

a. These procedures have been adopted to ensure that implementation of the Privacy Act does not have the unintended effect of denying individuals the benefit of congressional assistance which they request.

b. A disclosure under the above routine use does NOT require the employee's prior written consent. The congressional inquiry will be deemed to have been made "at the request of" the employee in the following cases:

(1) When the congressional inquiry includes a copy of a letter from the individual to whom the personnel record pertains.

(2) When the congressional inquiry indicates that the request is being made on the basis of a written request from the individual to whom the personnel record pertains.

(3) When the congressional office orally advises the personnel office that its request is being made on the basis of a written request from the individual to whom the personnel record pertains. (The personnel office shall verify all such requests.)

c. In cases where the congressional inquiry indicates that the request is being made on behalf of a person other than the individual whose personnel record is to be disclosed, the personnel office shall advise the congressional office that written consent is required. The personnel office should not contact the employee or applicant unless the congressional office requests it to do so.

d. Personnel offices can, of course, respond to many congressional inquiries without disclosing information contained in records subject to the Privacy Act.

e. Information from personnel records may also be disclosed in response to a congressional inquiry without written consent or operation of the routine use described in this paragraph in any of the following cases:

(1) If the information would be required to be disclosed under the Freedom of Information Act (paragraph 4-7 a).

(2) If the member requests that the response go directly to the individual to whom the personnel record pertains.

(3) Under the provisions of paragraphs 2-1c, e, h, i, and 6-5.

4-25. FEES.

a. Location of Schedules.

(1) Fees pertaining to personnel records covered by the Government-wide systems notices are described in Part 294 of the OPM regulations and are payable to the Treasury of the United States.

(2) Fees pertaining to other personnel records, such as the additional records authorized only for remote office supervisors discussed in paragraph 4-28b, are described in paragraph 2-16 and appendix 1 (note especially section 10.77(a) and (b)(1) of that appendix).

b. Policy on Charging Fees for Personnel Records. Since the OPM regulations do not REQUIRE the charging of fees in any instance, and appendix 1 states that no fee is to be charged for copies of personnel records provided to the employee or applicant to whom they pertain, fees will be charged only as follows:

(1) No fee will be charged for the FIRST copy of personnel records described in paragraph 4-25a(1). Fees will be charged for any subsequent copies furnished and charges will be in accordance with provisions of the OPM regulations.

(2) No fee will be charged for the FIRST copy of personnel records described in paragraph 4-25a(2). If additional copies are requested and, in the judgment of the system manager, the furnishing of additional copies involves unreasonable costs to the agency, advice shall be sought from AHR before they are furnished.

4-26. LEAVE CHARTS.

(FAA Form 3600-16, Leave Chart For Leave Year, or equivalent.) Random (rather than alphabetical) listing of employees' names, and management accessing by date (rather than personal identifier) is the proper use of posted leave charts. Under these circumstances the charts are NOT subject to the provisions of the Privacy Act. If the leave charts are posted either physically or electronically, the type of leave should not be indicated.

4-27. PERSONNEL MANAGEMENT INFORMATION SYSTEM (PMIS).

PMIS is covered by the OPM/GOVT-1 system notice.

SECTION 6. SUPERVISOR'S PERSONNEL RECORDS

4-28. AUTHORIZED SUPERVISOR's PERSONNEL RECORDS.

Only the following personnel records are authorized to be maintained by FAA supervisors. (See also paragraph 4-29)

a. Records Authorized for All Supervisors.

(1) **Confidential Statements of Employment and Financial Interests.** Statements are maintained by review officials identified in agency directives.

(2) **Agency System Grievances.** Records associated with an informal grievance are retained by the supervisor who replies to the grievance at the informal stage. These records are forwarded to the grievance official, if the employee later files a formal grievance. Records associated with a formal grievance are retained by the employee's grievance official identified in the agency directive on adverse actions, appeals, and grievances. When the grievance is decided, the complete grievance file is forwarded to the appropriate human resource management division.

(3) **Adverse Action Records.** Copies of proposed adverse actions are retained by supervisors authorized to propose actions. If the action is sustained, the material is forwarded, along with any employee's reply, to the appropriate human resource management organization for inclusion in the adverse action file. If not sustained, the proposed action and any employee's reply are destroyed.

(4) **Letters of Reprimand.** Copies are retained by the supervisor who signed the letters until the employees

concerned have had the opportunity to respond. If a letter is sustained, it is forwarded to the appropriate human resource organization to be placed in the employee's Official Personnel Folder (OPF). If a letter is not sustained, it is destroyed.

(5) Written Admonishments and Records of Oral Admonishments. Copies are retained by the supervisor taking the action. Records of such actions may be noted, or retained separately until they have served their purpose. Refer to Order 1350.15B, Records Organization, Transfer, and Destruction Standards.

b. Additional Personnel Records Authorized for Remote Office Supervisors. In addition to the personnel records authorized in paragraph 4-28a for all supervisors, FAA supervisors remote from the personnel office which keeps the OPFs of their subordinates, may maintain operating "personnel folders." ("Remote" means outside of the normal commuting area where the OPF is maintained and is to be defined by the appropriate human resource organization.) These folders are authorized ONLY for supervisors in remote offices OR for remote administrative field offices (which have been established under the provisions of Order 1100.5C, FAA Organization—Field) under the conditions and in accordance with the restrictions described in 5 CFR 293-31. ALTHOUGH AUTHORIZED, THE MAINTENANCE OF THESE RECORDS IS NOT ENCOURAGED. All supervisors should maintain only those personnel records which are absolutely essential for the conduct of official business and authorized by this order. Remote office personnel records include ONLY the following:

(1) Duplicate copies of employee's Performance Evaluation Records (also filed in OPF).

(2) Lists of employee's formal and informal training planned and accomplished.

(3) Notes on employee performance.

(4) Copies of employee's SF-171 and individual development plans.

(5) Information on employee's special qualifications and skills.

(6) Information on employee's performance on specific projects, details, or assignments.

(7) Notes on employee's recognition and awards material.

(8) Notes on employee's attendance and leave (which are separate from the time and attendance reporting and recordkeeping described in DOT/FAA 806, FAA Employee Payable System).

(9) Notes on employee's counseling sessions.

(10) Copies of debt complaint correspondence.

(11) Photocopies of SF-50's for employees.

(12) Copies of supervisor's responses to reference inquiries.

(13) Copies of employee's Personnel Security Action Request, FAA Form 1600-17, indicating the employee's security clearance.

(14) Other information on employee's experience, education, training, special qualifications and skills, position descriptions, performance appraisals and conduct.

4-29. GUIDANCE FOR SUPERVISORS.

Human resource organizations shall provide guidance to supervisors regarding preparation, maintenance, safeguarding, and disposition of records described in paragraph 4-28. This guidance will be consistent with the provisions of 5 FCR 293-31 and provisions of this order regarding the safeguarding of personnel records.

4-30. UNCIRCULATED PERSONAL NOTES.

Supervisors may retain personal notes and paper WHICH THEY HAVE AUTHORED. Although these are in the possession of the supervisor and used in performing official functions, they are not agency records for purposes of the Privacy Act unless circulated or used as the basis for an official agency decision. These do NOT include official records or reproductions of official records required or officially authorized to be used by the agency. Uncirculated personal notes are not subject to the control of the agency and are retained or discarded at the discretion of the supervisor. These notes are not subject to the provisions of the Privacy Act. However, if the notes are typed by, or made available to, any other person or office, the status is changed to that of a agency record.

CHAPTER 5. SAFEGUARDING PRIVACY ACT RECORDS

SECTION 1. GENERAL

5-1. PRIVACY ACT SECURITY REQUIREMENTS.

The Privacy Act of 1974 imposes numerous obligations upon FAA and each individual employee to prevent the misuse of personal information, ensure its confidentiality, and preserve its integrity. While the law does not establish specific security standards, it is clear that FAA is obligated to provide a reasonable degree of protection against accidental or deliberate unauthorized disclosure, destruction, or modification of personal data through the implementation of appropriate administrative, physical, and technical safeguards. The major portions of the Privacy Act (5 U.S.C., section 552a) which establish security as a primary privacy prerequisite are as follows:

a. Subsection (b), which limits disclosures of personal information only to authorized individuals and agencies;

b. Subsection (e)(5), which requires accuracy, relevance, timeliness, and completeness of records; and

c. Subsection (e)(10), which requires the use of safeguards to ensure the confidentiality and security of records.

The safeguard against unauthorized disclosure refers to any form of transfer of records covered under the Privacy Act. This would include the electronic as well as manual transmission of information. See section 3, paragraph 5-13(d) for guidance on the use of electronic mail with regard to Privacy Act information, and paragraph 5-6d for guidance on the use of FAX machines in the transmission of Privacy Act information.

5-2. SAFEGUARD SELECTION.

The technical requirements of the Privacy Act for safeguarding and ensuring the confidentiality, integrity, and security of personal data are less detailed and specific than some of the other provisions of the law. The level of security needed to support privacy depends on the uses which are made of the records, the uses which others could make of the records if inadvertently or intentionally disclosed, and the harm that might accrue to the subjects of the records if unauthorized release were to occur. In addition, security requirements are dependent on the operational and physical environment in which the system of records is used and stored. Safeguard selection must be tailored to address these varying considerations. The remaining two sections of this chapter prescribe minimum FAA security requirements for Privacy Act records. These should be read with the understanding that in many instances these safeguards will not be adequate to meet the protection standards established by the basic law for local conditions, and the presence of records having special sensitivity may require the establishment of a stronger security environment.

5-3. SECURITY RISK ASSESSMENT.

Risk analysis is a logical process which responsible record system managers may use to determine the necessary, yet reasonable level of security for records in their custody. This technique is equally applicable to the facilities having both manual and automated record systems. It is recognized that a formal risk analysis is not required at every FAA office, facility, or computer activity. The risk analysis processes provide record custodians with a better basis for deciding what security safeguards are necessary and reasonable to protect the particular type(s) of personal information for which they are responsible. The goal of risk analysis is to identify and prioritize those likely events which would compromise the integrity and confidentiality of personal data. The seriousness of a risk depends both on the potential impact of the event, its probability of occurrence, and the relative sensitivity of the data. Detailed guidelines for risk assessment is found in Order 1600.54B, FAA Automated Information Systems Security Handbook.

5-4 INSPECTIONS.

Supporting security elements shall include Privacy Act records protection as part of the facility security survey/inspection performed in accordance with Order 1600.2C, National Security Information, Order 1600.6C, Physical Security Management Program, Order 1600.54B, FAA Automated Information Systems Security Handbook, and other applicable directives. These inspections will be conducted to ensure that the security standards published in the description for each system are being implemented.

SECTION 2. PROTECTION OF MANUAL RECORDS SYSTEMS

5-5. INTRODUCTION.

This section establishes basic security standards for the protection of manual records covered by the Privacy Act of 1974, as amended.

5-6. REQUIRED SAFEGUARDS.

Working environments and operating procedures must be assessed to ensure that a reasonable degree of protection is provided for personal data subject to the Act. If there is a high concentration of records to protect, or if the sensitive nature of such records would make them more susceptible to efforts to gain unauthorized access, a higher degree of security should be instituted. Additional factors to be considered include the type of storage equipment, the environment in which it is located, frequency of checks made of the area, access controls in effect for the area, etc. The following constitute the minimum security standards for manual Privacy Act records held by FAA components.

a. **Records in Use.** Each employee working with hard copy records material containing personal data is fully responsible for its protection.

(1) It must not be left unattended outside the authorized storage area.

(2) It must be concealed from observation by unauthorized persons.

(3) It must not be verbally communicated to any unauthorized person.

(4) Correspondence or other material which include personal data extracted from the source material must be similarly safeguarded.

b. **Records in Storage.** As a minimum, records subject to the Privacy Act shall be stored in locked containers when unattended. Some of these are:

(1) Lockable filing cabinets for which there is a reasonable degree of certainty that unauthorized personnel do not possess keys.

(2) Lockable Lektrievers.

(3) Metal filing cabinets equipped with steel lock bars secured by GSA-approved changeable combination security padlocks.

(4) Any container which meets the requirements for storage of classified materials as specified in agency Order 1600.2C, National Security Information.

(5) A secured room equipped with the FAA locking system (key or combination) which is not left open after hours for cleaning purposes, and to which janitorial personnel and other unauthorized individuals do not have key access.

c. **Manual Transmission of Records.** Methods used for transmitting records subject to the Privacy Act shall protect the personal data from unauthorized disclosure. Externally, such records shall be transmitted in opaque envelopes, either in person, through the courier pouch system, or by U.S. mail. Within an office, personal information shall be placed in sealed envelopes conspicuously marked with the phrase, "TO BE OPENED BY ADDRESSEE ONLY." Records subject to the Privacy Act shall not be transmitted by other than approved secure systems.

d. **Automated Transmission of Records.** Regardless of method of transmission, automated or manual, all FAA employees or their designated contractors are responsible for protecting against unauthorized disclosure of Privacy Act information. Discretion needs to be used when transmitting any Privacy Act material. Do not transmit extremely sensitive Privacy Act information via FAX. In lieu of faxing, if time is critical, over-night mail service could be used. The proliferation of FAX machines has increased the chances of inadvertent, unauthorized disclosure of Privacy Act information. The possibility of misdialing could send the material to some other office or even directly into the wrong computer. Also, even if dialed and transmitted correctly, once received, it is likely to remain exposed and unattended while awaiting for pickup. In order to avoid such vulnerability if Privacy Act information must be faxed, the preferred method is to use secured fax equipment. If secured equipment is not available, the following information as outlined by the Office of Civil Aviation Security Operations, Investigations and Security Division, ACO-300, should be followed:

(1) The originating office calls the destination office to establish voice contact and informs them that a Privacy Act document is to be sent.

(2) Without breaking the voice connection, load a test sheet, blank sheet, and the Privacy Act document on the facsimile machine so that the test sheet and blank page are transmitted first.

(3) Begin sending the test sheet and ask the destination office to verify receipt of the test.

(4) Once verbal confirmation is received on the test sheet, the originating office can then terminate voice contact and allow the document to continue to transmit until complete.

(5) If the destination office says they are not receiving the test, and the blank page is starting to transmit, terminate the facsimile transmission and verify the facsimile phone number.

(6) Repeat steps 2 through 5 as required until transmission of the Privacy Act document is completed.

(7) If the receiving office needs to deliver the message to another person, the "For Official Use Only" envelope, FAA Form 1360-39, can be used.

e. **Reproduction.** Records subject to the Privacy Act shall not be reproduced without express permission of the local systems manager. Methods used for reproduction of such material shall preclude its exposure during the reproduction process.

f. **Destruction.**

(1) General Guidelines. Destruction of information governed by the Privacy Act is the responsibility of the offices having custody of this material and will be accomplished in accordance with instructions and schedules for the disposal of this material. Refer to Order 1350.15B, Records Organization, Transfer, and Destruction Standards. The requirement for destruction of manual records includes documents, paper waste products, and computer generated hard copy reports. As a general rule, destruction will be sufficiently thorough so that reconstruction or recovery of the information from the residue is not possible. The test that should be applied by responsible officials is whether or not the uncontrolled release of the information could result in SUBSTANTIAL harm, unfairness, or embarrassment to the subject. Information meeting this standard should be destroyed by using the means prescribed below even though it is not included in one of the identified record systems. The majority of the Privacy Act records may be disposed of by locally determined methods such as tearing or shredding which meets the spirit and intent of the law.

(2) Special Destruction Requirements. Material included in the record systems listed below has been identified by the system manager as being particularly sensitive. Consequently, paper materials from these systems will be destroyed by burning, pulping, pulverizing, chopping, or shredding.

(a) DOT/FAA 847, General Air Transportation Records on Individuals.

(b) DOT/FAA 806, FAA Employee Payable System.

(c) DOT/FAA 810, Discrimination Complaint Files.

(d) DOT/FAA 811, Employee Health Record System.

(e) DOT/FAA 813, Civil Aviation Security System.

(f) DOT/FAA 814, Equal Employment Opportunity Minority/Female Statistical Reporting System.

(g) DOT/FAA 815, Investigative Record System.

(h) All personnel records.

(3) Destruction of Computer-Media is to be carried out in accordance with the guidelines in FAA Order 1600.54B, FAA Automated Information Systems Security Handbook

5-7. IDENTIFYING PERSONNEL AUTHORIZED ACCESS.

Effective procedures shall be established to ensure that access to records is restricted to only authorized individuals.

5-8. LOCAL SECURITY PLAN CHECKLIST.

The following checklist is provided for use by responsible record custodians in developing local security plans for the protection of personal data contained in manual record systems. Additional assistance for unique problems may be obtained from the servicing security element.

a. Identify the records systems in which the personal data is included, and how it is received, processed, stored, accessed, transmitted, destroyed, retired, etc.

b. Prescribe responsibility for designating who is authorized to have access to what specific categories of personal data concerned.

c. Provide measures by which authorized users are positively identified.

d. Establish methods by which users are limited to the data to which they are entitled.

e. Provide appropriate protective measures for all incoming material containing personal data.

f. Establish controls needed for protection of the materials which are in use within the activity such as, access controls, access monitoring, isolation of work stations, special handling procedures, etc.

g. Prescribe storage requirements which properly protect the records during duty and non-duty hours, including such supplemental security safeguards as warranted by the nature of the information and by the local situation. (Minimum of locked files and/or storage rooms with effective key or combination controls. For more stringent pro-

tection, such measures as safe files, vault rooms, intrusion alarms, etc., may be prescribed.)

h. Specify methods of transmittal of personal data concerned either within or outside the activity to ensure its proper protection.

i. Provide destruction methods for waste material or access records which contain personal data (obsolete records, typing waste copies and carbons, shorthand notes, reproduction waste, etc.).

j. Prescribe emergency procedures and responsibilities for protection of the records when emergency situations arise (fire, tornado, civil disorder, earthquake, etc.).

k. Prescribe responsibility for monitoring compliance with the security plan.

l. Provide actions on identified violations of the security plan and for corrections on instances of mishandling of the information.

5-9. KEY CONTROL.

Keys to locks used in the protection of records shall be afforded a degree of protection commensurate with the sensitivity of the records. Under no circumstances will keys be maintained in unlocked desk drawers or file cabinets or hidden in the office for convenience or expediency. Controls should be established to ensure retrieval of keys when no longer required.

SECTION 3. SAFEGUARDING AUTOMATED RECORDS

5-10. GENERAL.

There are three categories of technical safeguards relevant to automated record systems (mainframes and personal computers). These are physical security measures, information management practices, and computer system/network security controls. Neither category by itself is likely to offer sufficient protection against the various threats to data confidentiality and integrity, but a well balanced, cost-effective program can be created by careful selection of appropriate safeguards from all three categories. Risk analysis, as an aide in the safeguard selection process, is particularly effective given the complexities of existing computer systems. Additional guidance beyond that contained in the following paragraphs is set forth in Order 1600.54B, FAA Automated Information Systems Security Handbook, and 36 CFR Part 1234, Electronic Records Management, published in the Federal Register, May 8, 1990.

5-11. PHYSICAL SECURITY.

Physical security measures are the first and most cost-effective line of defense against risks which stem from uncertainties in the physical environment as well as the unpredictability of human behavior. A good physical security environment is achieved through the judicious use of locks, barriers, etc., which are enforced with appropriate administrative sanctions. Another related item is to ensure equipment against damage from accident, fire, and other environmental hazards. The following basic physical security controls shall be instituted at FAA facilities which process information covered by the Privacy Act.

a. **Entry Controls.** Positive personnel access controls will be established to ensure that only authorized personnel have access to computer equipment rooms, remote terminal areas, media libraries, and other sensitive areas not within the confines of the central computer facility.

b. **After Hours Security.** Those areas specified above which are not occupied after normal duty hours will be secured to prevent unauthorized entry.

c. **Protection of Data.** Access to media libraries shall be restricted so as to minimize the number of personnel who enter a library or have access to containers housing source, object, or data files. Tapes, disks, CD ROM, etc., which contain particularly sensitive personal information may be further protected by being placed in locked containers or safes.

d. **Protection of Source Input and Output Documents.** An appropriate combination of physical and procedural controls should be established to protect such materials from theft, loss, or alteration. Computer generated output containing Privacy Act data shall be safeguarded in the ADP facility to prevent unauthorized dissemination or acquisition. The responsibility for protecting this material passes to the user upon delivery or receipt.

e. **Environmental Safeguards.** The vulnerability of the facility and the records housed within it to damage or destruction from fire, flood, etc., should be considered in establishing the physical security program. A related concern is the existence of well-coordinated and tested plans that will permit continued processing of essential data without unacceptable delays.

5-12. INFORMATION MANAGEMENT PRACTICES.

This category of safeguards refers to those procedures, administrative controls, and managerial policies used to control the many operations performed on information during the data processing cycle. These managerial controls

are also required to support physical and system-based controls implemented to achieve the objectives of the Privacy Act. Soundly developed and administered managerial controls are essential to maintain the accuracy and integrity of personal data. Controls in this category include:

a. Restrictions on internal facility handling and control of personal data.

b. Requirements to maintain records to trace disposition of personal data.

c. Operational data processing controls.

d. Secure programming practices.

e. Procedural auditing.

5-13. SYSTEM AND NETWORK SAFEGUARDS.

Once adequate physical security and administrative controls have been established, the need for system-based controls should be considered. Such protective measures are particularly applicable to large-scale interactive systems where the threats to data security are more complex. The potential of intentional and accidental compromise increases with the amount of data accessible, the number of possible users of that data, and the geographic distribution of the network. Some applicable security controls in this area of concern are as follows:

a. **User Identification and Authentication.** The identification and validation of users who use an interactive system for access to individual data files is a basic prerequisite to establishing adequate system level security controls. Not only do identification and access controls prevent unauthorized users from entering the system, they also control the ability of legitimate users to read, alter, or destroy data.

b. **Access Auditing.** The ability to account for who has had access to which data may be required if the information is particularly sensitive. Data usage reports, also known as audit trails, can be generated to provide as little or as much of this information as needed to ensure that unauthorized access is detected when it occurs.

c. **Transmission Security.** Under certain conditions, the use of data encryption techniques may be needed to provide additional protection to highly sensitive information introduced into remotely accessed computer systems. Federal Information Processing Standard #46, "Data Encryption Standard," specifies an algorithm to be implemented in electronic hardware devices and used for the cryptographic protection of computer data. Requests for the use of this technique within FAA must be approved by the Assistant Administrator for Civil Aviation Security, ACS-1.

d. **Electronic Mail Security.** The use of electronic mail to transfer information covered under the Privacy Act leaves that information extremely vulnerable to inadvertent or intentional disclosure, and therefore, is to be avoided. The transfer of Privacy Act information in the body of an electronic mail message, or the attachment of a Privacy Act record to an electronic mail message, allows that information to be forwarded to other, possibly unauthorized personnel, or to be printed out and left visible for unauthorized personnel to see. Since the capabilities of electronic mail are expanding faster than the guidance on its uses, the vulnerability of Privacy Act and other sensitive information is caught in the middle. Applying the mandates of the Privacy Act itself, in its subsection (b) which limits disclosures of personal information, and subsection (e)(10) which requires the use of safeguards to ensure the confidentiality and security of records, and pending other official guidance from OMB on the use of electronic mail with regard to Privacy Act information, this guidance will prevail. Remembering in this restriction that Privacy Act information includes, but is definitely not limited to, name, home address, home phone number, social security number, medical information, security files, civil rights actions, and certain personnel actions.

5-14. NEW SYSTEMS OR MAJOR CHANGES TO EXISTING SYSTEMS.

The Privacy Act requires all agencies to provide Congress and the Office of Management and Budget (OMB) with advance notice of the creation of a new or major modification of an existing record system used to process personal information. The purpose of such notification is to permit an independent privacy impact assessment to be made of the proposed system. The presence or absence of security and confidentiality safeguards constitute important elements in the approval review of a new or extensively modified system. The security/safeguard sections of these notices shall be coordinated with the FAA ADP Security Program Manager, ACO-320, in the office of the Assistant Administrator for Civil Aviation Security, before submission to Congress and OMB.

CHAPTER 6. EXEMPTIONS AND SPECIAL SITUATIONS

6-1. GENERAL EXEMPTIONS.

The Act permits the head of an agency to publish rules exempting any system of records from certain provisions of the Act, if the system of records is maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws. All system descriptions whether exempt or not, must be published in the Federal Register.

6-2. SPECIAL EXEMPTIONS.

The Act also provides that the head of the agency may exempt a system of records from certain requirements of the Act if the system of records consists of:

a. Material required to be kept secret by Executive Order in the interest of national defense or foreign policy.

b. Investigatory material compiled for law enforcement purposes. However, if any individual is denied any right, privilege, or benefit that he would otherwise be entitled to by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, it shall be provided to the person, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an expressed promise that the identity of the source would be held in confidence, or, prior to September 27, 1975, under an implied promise that the source's identity would be held in confidence.

c. Records maintained in connection with providing protective services to the President of the United States or other individuals pursuant to section 356 of Title 18.

d. Records required by statute to be maintained and used solely as statistical records.

e. Investigatory material compiled solely to determine suitability, eligibility, or qualification for Federal civilian employment, military service, Federal contracts, or access to classified information, but only to the extent the disclosure of such material would reveal the identity of a source who furnished the information under an express promise that the identity of the source would be held in confidence, or prior to September 27, 1975, under an implied promise that the identity of the source would be held in confidence.

f. Testing or examination material used solely to determine individual qualifications for appointment or promotion in Federal service, the disclosure of which would compromise the objectivity or fairness of the testing or examination process.

g. Evaluation material used to determine potential for promotion in the armed services. This applies only to the extent the disclosure of such material would reveal the source of the information furnished under an express promise that the identity of the source would be held in confidence, or prior to September 27, 1975, under an implied promise that the identity of the source would be held in confidence.

6-3. PROCEDURES FOR EXEMPTING SYSTEMS OF RECORDS.

The normal procedures for publishing rules apply to publishing specific and general exemptions. The notice to be published in the Federal Register must specify the name of the system, the specific provisions of the Act from which the system is to be exempted, and the reasons for the exemption. Any office, service, region, or center proposing to exempt a system of records should consult with AIT-400 and the Office of the Chief Counsel or the Regional or Center Assistant Chief Counsels, as applicable.

6-4. GOVERNMENT CONTRACTORS.

The provisions of the Act apply to: (1) contracts awarded prior to September 27, 1975, which provide for design, development, and/or operation of a system of records on individuals for an agency function, and (2) contracts initiated on or after September 27, 1975, which may involve such systems of records even when those systems are not specifically identified in the particular contractual statement of work. Any contractor or employee thereof shall be considered an FAA employee for purposes of the criminal penalties provision of the Act, if such contract is agreed to on or after September 27, 1975. Note that state and local governments and agencies performing an agency function under an agreement with FAA are considered to be contractors for this purpose. FAA shall develop and include, in contracts providing for the use or establishing of systems of records in support of an agency function, appropriate contract clauses to implement the requirements of the Act. Such clauses shall include language regarding the criminal penalties for willful disclosure and appropriate references to the agency's implementing regulations. These provisions apply to any contractor serving as the collector, analyzer, or processor of data under grants or contracts to support FAA programs.

6-5. STATISTICAL RECORDS.

a. General. This category of disclosure requires additional emphasis in that many of FAA's systems of records fall within the scope of records used solely as statisti-

cal research or reporting records and are transferred in a form that is not individually identifiable.

b. Procedure.

(1) Records disclosed pursuant to this provision must be stripped of individual identifiers. In addition, the system manager must ensure that the identity of individuals cannot be reasonably deduced from the records including tabulations or other data in the requester's possession or in combination with various statistical records readily available.

(2) Records may be disclosed for statistical research or reporting purposes only after the system manager has received and evaluated a written statement which indicates the need and certifies that it will only be used for statistical purposes.

(3) In addition to the foregoing, the system manager must ascertain that the information disclosed is not to be used in any way to make determinations regarding an individual or to either confirm or deny any benefit to the individual.

CHAPTER 7. REPORTS

7-1. NEW OR REVISED SYSTEMS OF RECORDS (RIS: 1280-3).

a. A report shall be submitted to the IT Information Management Division, AIT-400 for each new system of records and for changes to existing systems. The criteria for determining what constitutes a change to an existing system requiring the preparation of the report are as follows:

(1) An increase or change in the number or types of individuals on whom records are maintained.

(2) An increase in the type or categories of information maintained.

(3) A change in the manner in which the records are organized or the manner in which the records are indexed or retrieved so as to change the nature or scope of those records.

(4) A change in the purposes for which the information is used.

(5) A change in the equipment configuration (i.e., hardware and/or software) on which the system is operated so as to create the potential for either greater or easier access; e.g., adding a telecommunications capability.

(6) Additions or deletions to the list of routine uses.

b. The Washington headquarters office and service directors, and region and center heads shall submit the required information for all new or revised systems of records to the Operational Privacy Act Coordinator, AIT-400, at least 120 days prior to the implementation of the proposed new or revised system in order for the request to be forwarded to OST for signature and then to OMB at least 90 days prior to implementation.

c. The Operational Privacy Act Officer shall review the submissions to determine compliance with the requirements. These requirements are contained in Office of Management and Budget Circular No. A-130. Upon review and approval, letters of submission, enclosing the narrative statement and the description of the new or revised systems of records, shall be prepared for the approval and signature of the Assistant Secretary for Administration, M-1.

d. The approved new or revised systems of records shall be submitted to the Chairman of the Committee on Governmental Affairs of the United States Senate, the Chairman of the House Committee on Government Operations, and the Office of Information and Regulatory Affairs, Office of Management and Budget, and published in the Federal Register. These individuals/offices are afforded 40 days to react to proposed new or revised systems of records before these systems can be used.

7-2. CANCELLATION OF SYSTEMS OF RECORDS.

a. Cancellation of any existing FAA system of records shall be initiated by or coordinated with the appropriate system manager. A statement shall be provided to the Operational Privacy Act Coordinator, AIT-400, stating the reasons for cancellation and the recommended effective date.

b. The FAA Operational Privacy Act Coordinator shall prepare a letter for the signature of the Assistant Secretary for Administration to the Office of Management and Budget explaining the reason for the cancellation. Final action for cancellation will occur following OMB concurrence.

7-3. PRIVACY ACT STATISTICAL SUMMARY (RIS: 1280-2).

To ensure compliance with the guidelines cited in the Privacy Act, 5 U.S.C., section 552a(s), OMB requires a biennial (every 2 years) statistical report of Privacy Act–related activities regarding all systems of records. In order to comply with the guidelines set forth in OMB Circular A-130, appendix I, paragraph 4a, each system manager or delegate will need to keep a log of requests from individuals for access to or requests for amendment of records about themselves in systems of records that cite the Privacy Act in support of their requests. Each Privacy Act coordinator in an office, service, region, or center with a Privacy Act system of records is responsible for collecting separate data for each year of the reporting cycle on FAA Form 1280-1, and submitting it to the Operational Privacy Act Coordinator, AIT-400. The date of the report will be by the end of April of the second year. The biennial cycle is 1992 and 1993, 1994 and 1995, etc. (See OMB Circular A-130, appendix I, paragraph 4a, for more detail on what is required.) At the time of the data call, any additional guidance provided by OMB will be relayed to the Privacy Act coordinators in the offices, services, regions, and centers.

APPENDIX 1. FEES

DEPARTMENT OF TRANSPORTATION

Office of the Secretary of Transportation
49 CFR Part 10, Subpart H - Fees

§10.71 General.

This subpart prescribes fees for services performed for the public under this part by the Department.

§10.73 Payment of fees.

The fees prescribed in this subpart may be paid by check, draft, or postal money order payable to the Treasury of the United States.

§10.75 Fee schedule.

(a)	*Copies of documents by photocopy or similar method:*	
	Each page not larger than 11 x 17 inches:	
	First page	*$.25*
	Each page	*.05*
(b)	*Copies of documents by typewriter: Each page*	*2.00*
(c)	*Certified copies of documents:*	
	(1) With Department of Transportation seal	*3.00*
	(2) True copy, without seal	*1.00*
(d)	*Photographs:*	
	(1) Black and white print (from negative)	*1.25*
	(2) Black and white print (from print)	*3.15*
	(3) Color print (from negative)	*3.50*
	(4) Color print (from print)	*6.25*
(e)	*Duplicate data tapes—each reel of tape or fraction thereof*	*36.00*

The applicant must furnish the necessary number of blank magnetic tapes. The tapes must be compatible for use in the supplier's computer system, 1/2 inch wide and 2,400 feet long, and must be capable of recording data at a density of 556 or 800 characters per inch. Unless otherwise designated, the tapes will be recorded at 556 CPI density. The Department of Transportation is not responsible for damaged tape. However, if the applicant furnishes a replacement for a damaged tape, the duplication process is completed at no additional charge.

(f)	*Micro reproduction fees are as follows:*	
	(1) Microfilm copies, each 100 foot roll or less	*$3.75*
	(2) Microfiche copies, each standard size sheet (4" x 6" containing up to 65 frames)	*.15*
	(3) Aperture card to hard copy, each copy	*.50*
	(4) 16mm microfilm to hard copy:	
	First	*.25*
	Additional	*.07*
(g)	*Computerline printer output, each 1,000 lines or fraction thereof*	*1.00*

§10.77 Services performed without charge.

(a) No fee is charged for time spent in searching for records or reviewing or preparing correspondence related to records subject to this part.

(b) No fee is charged for documents furnished in response to:

(1) A request from an employee or former employee of the Department for copies of personnel records of the employee;

(2) A request from a member of Congress for official use;

(3) A request from a State, territory, U.S. possession, county or municipal government, or an agency thereof;

(4) A request from a court that will serve as a substitute for the personal court appearance of an officer or employee of the Department;

(5) A request from a foreign government or an agency thereof, or an international organization.

(c) Documents are furnished without charge or at a reduced charge, if the Assistant Secretary of Administration or the Administrator concerned, as the case may be, determines that waiver or reduction of fees is in the public interest, because furnishing the information can be considered as primarily benefiting the general public.

(d) When records are maintained in computer-readable form rather than human-readable form, one printed copy is made available which has been translated to human-readable form without charge for translation but in accordance with 10.75(g) regarding computer line-printed charges.

OFFICE OF PERSONNEL MANAGEMENT OPM

5 C.F.R. Part 294

§294.109 Fees.

(a) *Applicability of fees.* OPM entities will furnish, without charge, reasonable quantities of materials that they have available for free distribution to the public. Subject to payment of fees as specified in this section, OPM may furnish other material. These fees are intended to recoup the full allowable direct costs of providing services.

(b) *Payment of fees.* Individuals may pay fees by check or money order, payable to the Office of Personnel Management.

(1) OPM will not assess fees for individual requests if the total charge would be less than $25, except as provided in paragraph (b)(5) of this section.

(2) If a request may reasonably result in a fee assessment of more than $25, OPM will not release records unless the requester agrees to pay the anticipated charges.

(3) If the request does not include an acceptable agreement to pay fees and does not otherwise convey a willingness to pay fees, OPM will promptly provide notification of the estimated fees. This notice will offer an opportunity to confer with OPM staff to reformulate the request to meet he requester's needs at a lower cost. Upon agreement to pay the required fees, OPM will further process the request.

(4) As described in 294.107, OPM ordinarily responds to Freedom of Information Act requests in a decentralized manner. Because of this, OPM may at times refer a single request to two or more OPM entities to make separate direct responses. In such cases, each responding entity may assess fees as provided by this section, but only for direct costs associated with any response the component has prepared.

(5) OPM may aggregate requests and charge fees accordingly, when there is a reasonable belief that a requester, or a group of requesters acting in concert, is attempting to break a request down into a series of requests to evade the assessment of fees.

(i) If multiple requests of this type occur within a 30-day period, OPM may provide notice that it is aggregating the requests and that it will apply the fee provisions of this section, including any required agreement to pay fees and any advance payment.

(ii) Before aggregating requests of this type made over a period longer than 30 days, OPM will assure that it has a solid basis on which to conclude that the requesters are acting in concert and are acting specifically to avoid payment of fees.

(iii) OPM will not aggregate multiple requests on unrelated subjects from one person.

(6) If fees for document search are authorized as provided in paragraph (f) of this section, OPM may assess charges for an employee's (or employees') time spent searching for documents and other direct costs of a search, even if a search fails to locate records or if records located are determined to be exempt from disclosure.

(7) Services requested and performed but not required under the Freedom of Information Act, such as formal certification of records as true copies, will be subject to charges under the Federal User Charge Statute (31 U.S.C., section 483a) or other applicable statutes.

(c) *Payment of fees in advance.* If OPM estimates or determines that fees are likely to exceed $250, OPM may require the payment of applicable fees in advance.

(1) If an OPM official, who is authorized to make a decision on a particular request, determines that the requester has a history of prompt payment of FOIA fees, OPM will provide notice of the likely cost and obtain satisfactory assurances of full payment.

(2) When a person, or an organization that a person represents, has previously failed to pay any fee charged in a timely manner, OPM will require full payment in advance. In this section, an untimely payment is considered to be a payment that is not made within 30 days of the billing date.

(3) OPM will not begin to process any new request for records, if a person, or an organization that a person represents, has not paid previous fees, until that individual has paid the full amount owed plus any applicable interest and made a full advance payment for the new request.

(4) If a request, which requires the advance payment of fees under the criteria specified in this section, is not accompanied by the required payment, OPM will promptly notify the requester that he or she must pay the required fee within 30 days and that OPM will not further process the request until it receives payment.

(5) OPM may begin assessing interest charges on an unpaid bill starting on the 31st day following the date on which the bill was sent. Interest will be at the rate prescribed in 31 U.S.C., section 3717 and will accrue from the date of the billing.

(6) To encourage the repayment of debts incurred under this subpart, OPM may use the procedures authorized by Pub. L. 97-365, the Debt Collection Act of 1982. This may include disclosure to consumer reporting agencies and the use of collection agencies.

(d) *Waiver of fees.* OPM will furnish documents under this subpart without any charge, or at a reduced charge, if disclosure of the information is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the Government, and is not primarily in the commercial interest of the requester.

(1) Anyone who asks for waiver of fees under this section, must explain why he or she is entitled to a waiver. The explanation must be in sufficient detail to allow OPM to make an informal decision on the waiver request. A statement that essentially quotes section 552(a)(4)(A)(iii) of the Freedom of Information Act or the provisions of this section, does not satisfy this requirement. An OPM official may deny a waiver of fees without further consideration if the required explanation is not provided.

(2) A requester may appeal the denial of a waiver request as provided by 294.110.

(e) *Rates used to compute fees.* The following rates form the basis for assessing reasonable, standard charges for document search, duplication, and review as required by 5 U.S.C., section 552(a)(4). The listing of rates below should be used in conjunction with the fee components listed in paragraph (f) of this section, the first-100-pages of paper copies exception in paragraph (g) of this section, and the first-2-hours manual records search exception in paragraph (h) of this section.

Employee time	*Salary rate plus 16% to cover benefits.*
Photocopies (up to 8 1/2" x 14")	*$0.13 a page.*
Printed materials, per 25 pages or fraction thereof	*$0.25.*
Computer time	*Actual direct cost.*
Supplies and other material	*Actual direct cost.*
Other costs not identified above	*Actual direct cost.*

(f) *Fee components by category of user.* For the purpose of assessing fees under this section, requests may have three cost components. These are the cost of document search, the cost of duplication, and the cost of review. When computing the fee applicable to a request, OPM will apply the rates in paragraph (e) of this section, to the cost components that apply to the requesters category. Cost components apply to categories of requesters as follows:

(1) A commercial use requester—Pays actual direct costs for document search, duplication, and review.

(2) A requester from an educational and non-commercial scientific institution and a representative of the news media—Pays actual direct costs for document duplication when records are not sought for commercial use. (Requesters in this category do not pay for search and review.)

(3) All other requesters—Pay actual direct costs for document search and duplication. (Requesters in this category do not pay for review.)

(g) *First 100 pages of paper copies.* There will be no charge to categories of requesters included in paragraphs (f)(2) and (3) of this section for the first 100 pages of paper copies, size 8 1/2" by 11" of 11" by 14" or for a reasonable substitute for this number of copies. An example of a reasonable substitute is a microfiche containing the equivalent of 100 pages.

(h) *First 2 hours of manual records search.* OPM will not charge requesters in the "all other" category for the first 2 hours of manual records search. If a person asks for records from a computerized data base, OPM will use the following formula, promulgated by the Office of Management and Budget, to provide the equivalent, in computer records search time, of 2 hours of manual records search.

(1) OPM will add the hourly cost of operating the central processing unit that contains the record information to the operator's hourly salary plus 16 percent.

(2) When the cost of a search (including the operator's time and the cost of operating the computer to process a request) equals the equivalent dollar amount of 2 hours of the salary of the person performing the search (i.e., the operator), OPM will begin assessing charges for computer search.

APPENDIX 2.
INDEX

	Para. No.	*Page No.*
ACCESS	2-3	12
Appeals	2-8, 2-9	15
Denial of Access	2-12, 4-12	17, 34
Exempted	2-4	13
Fees	2-16	18
In Person	2-5	13
Mail Requests	2-4	13
Method	2-3	12
Amendment	2-7	14
ADVERSE DETERMINATIONS	2-13	17
CONGRESSIONAL INQUIRIES	4-24	38
CRIMINAL PENALTIES AGAINST EMPLOYEES	2-15	17
COLLECTION OF INFORMATION	3-1	23
CONTRACTORS	6-4	55
CORRECTIONS OF RECORDS	2-7	14
DEATH	2-6a (note), 4-7c(1)	14,32
DEFINITIONS	1-7, 4-3	2, 31
DENIALS		
Anticipation of Civil Proceeding	2-4	13
Appeals	2-8	15
Exempt from Access	2-4a, 2-5a	13
Right to Appeal	2-8	15
DISCLOSURE		
Accounting of	3-8, 4-8	25, 32
Exclusion from	3-8a	25
Personnel Records (some exempt)	4-8	32
Procedures	3-8c	26
Requirements	3-8b	25
Compulsory Legal Process	3-4	24
Conditions	2-1, 4-7	11, 32
Defined	1-7e	2
E-Mail	5-13d	51
False Pretenses	2-15c	17
Third Party Requests	2-6	14
Unauthorized	2-15a	17
E-MAIL SECURITY	5-13D	51
EXEMPTIONS	6-1, 6-2	55
FEES	2-16, Appendix 1	16
Personnel Records	4-25	39
FOIA REQUIRED RELEASE	4-7a	32
FOIA VS PRIVACY ACT	2-3a(1)	12
IDENTIFICATION VERIFICATION	2-4b(1)	13
MEDICAL RECORDS RELEASE	2-4b(3)	13
	2-5b(3)	13
MATCHING PROGRAMS	3-5	24
NOTICES, GOVERNMENT WIDE SYSTEMS OF	4-25a(1)	39

INDEX (Continued)

	Para. No.	*Page No.*
PERSONNEL RECORDS	4-1	31
Access	4-11	33
Amendment	4-13	34
Annual Review Announcement	4-18	37
Confidential Employment Vouchers	4-21	38
Congressional Inquiries	4-24	38
Correction of Records	4-13	34
Denial of Access	4-12	34
Disclosure	4-7	32
Fees	4-25	39
FOIA Required Release	4-7a	32
Grievance, Arbitration, and Unfair Labor Practice/Change Complaint Files	4-20d	37
Leave Charts	4-26	39
Medical Records	4-20e	38
PMIS	4-27	39
MPP (Merit Promotion Plan)	4-20b	37
MPP Privacy Act Statement	4-23	38
Privacy Act Statements	3-2a	23
Reference Inquiries	4-22	38
Safeguarding	4-19	37
Suitability Files	4-20a	37
Supervisor's Personnel Records	4-28 & 29	39 & 40
Uncirculated Personal Notes	4-30	40
PRIVACY ACT STATEMENTS	3-2	23
What an Employee Can do—Civil Remedies Corrections	2-10 thru 2-14	16 & 17
Criminal Penalties	2-15	17
PRIVACY VS. FOIA	1-9e, 2-1b, 2-3a(1)	4, 11, 12
PROCEDURES FOR COLLECTING INFORMATION	3-2	23
PUBLIC NOTICE		
Failure to Publish	2-15b	17
RECORDS		
Safeguards	5-1 thru 5-14	47-51
Supervisor	4-28 thru 4-30	39-41
Systems of Records	3-1 thru 3-8	23-26
Automated	5-6d	48
	5-10 thru 5-14	50-51
Manual	5-6c	48
REGULATIONS		
OMB and CFR	2-12a	17
	4-5 & 6	31
	Appendix 1	1-5
REPORTS		
New or Revised Systems of Records	7-1	57
Privacy Act Statistical Summary	7-3	57
Cancellation	7-2	57

RESPONSIBILITIES
FAA Employees 1-10k 5
Privacy Act Coordinator ..... 1-7f, l, m, and n 2
1-10i 5
2-6a 14
2-7a 14
SAFEGUARDS 3-6 25
5-2 47
SOCIAL SECURITY NUMBERS 1-9h, 3-2b 4, 23
STATISTICAL RECORDS 6-5 56
THIRD PARTY REQUESTS OR THIRD PARTY PRESENT
OR COMMENTING ..... 1-9a, 2-1h, 2-3b, 2-5b(3), 2-6 3,4,12,13,14
TIME LIMITS
Access 2-4b 13
Third Party Request 2-6a 14
Corrections 2-7 14
Personnel Records 4-13c 36
Appeals ..... 2-8c & d, 2-9 15
WAIVERS ..... Appendix 1 2