

CHANGE**U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION****ORDER 1280.1B
CHG 1**

National Policy

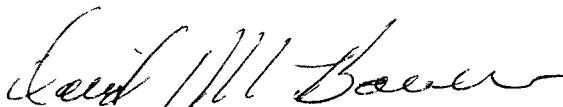
Effective Date:
08/16/2011**SUBJ: Protecting Personally Identifiable Information (PII)**

1. **Purpose.** The purpose of this change is to implement the Line of Business and Staff Office Privacy Manager duties and responsibilities for Order 1280.1B Protecting Personally Identifiable Information.
2. **Who this change affects.** This change applies to all FAA employees, contract personnel, and others who have authorized access to FAA information resources. "Others" include grantees, consultants, licensees, and any person or entity, domestic or foreign, having a formal agreement with the FAA.
3. **Explanation of Changes.** To change the title Privacy Coordinator to Privacy Manager, as well as clarify the duties and responsibilities of the Privacy Manager which will be outlined in chapter 2 paragraph k of the Order 1280.1B.
4. **Disposition of Transmittal Paragraph.** Retain this transmittal sheet until the directive is cancelled or superseded.

PAGE CHANGE CONTROL CHART

| Remove Pages | Dated | Insert Pages | Dated |
|--------------|----------|--------------|----------|
| 9 through 11 | 12/17/08 | 9 through 11 | 08/16/11 |

5. **Administrative Information.** This Order change is distributed to divisions and branches in Washington headquarters, regions, and centers and to all field offices and facilities.



David Bowen
Assistant Administrator for
Information Services and Chief Information Officer



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

ORDER
1280.1B

Effective Date:
12/17/2008

SUBJ: Protecting Personally Identifiable Information (PII)

1. This order prescribes the Federal Aviation Administration (FAA) Policy for Protecting Personally Identifiable Information about individuals. This directive establishes policy, delegates authority, and assigns responsibility for ensuring compliance with this order within each organization.
2. This version of FAA Order 1280.1 implements the various privacy laws based on the Privacy Act of 1974 (the Privacy Act), the E-Government Act of 2002 (Public Law 107-347), the Federal Information Security Management Act (FISMA), Department of Transportation (DOT) privacy regulations, Office of Management and Budget (OMB) mandates, and other applicable DOT and FAA Records Management procedures and guidance. The FAA Privacy Officer position is located within the Office of the Assistant Administrator for Information Services (AIO-1) and Chief Information Officer (CIO).
3. 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, transmitting, sharing, and disseminating personal information.
4. The objective of this order, in its format and content, is to provide a single reference source that incorporates all higher level policy guidance for the protection of Personally Identifiable Information (PII) and privacy records within the FAA.
5. Upon issuance, this Order does not address the budget impact to lines of businesses and staff offices to implement this order. Each LOB/SO CIO's must develop an implementation plan and budget requirements within one year of issuance of this Order. Once the budget requirements to implement this order are developed, the LOB/SO CIO's must submit that request to their organizational budget office for funding. With the receipt of that funding, the LOB/SO is required to fully exercise their implementation plan.

A handwritten signature in black ink, reading "David M. Bowen", is positioned above the printed name.

David Bowen
Assistant Administrator for
Information Services and Chief Information Officer

Table of Contents

| <i>Paragraph</i> | <i>Page</i> |
|---|-------------|
| Chapter 1. General Information | |
| 1. Purpose of this Order | 1 |
| 2. Who This Order Affects..... | 1 |
| 3. Where Can I Find This Order?..... | 1 |
| 4. What This Order Cancels..... | 1 |
| 5. Explanation of Policy Changes..... | 1 |
| 6. Scope..... | 1 |
| 7. Background..... | 2 |
| Chapter 2. Roles and Responsibilities | |
| 1. Roles and Responsibilities | 3 |
| 2. Other Roles and Responsibilities..... | 10 |
| 3. Delegation of Authority | 10 |
| Chapter 3. Policy | |
| 1. Requirements | 12 |
| 2. Disclosure and Access to Records | 13 |
| 3. Collection and Maintenance of Systems of Records | 14 |
| 4. Safeguarding Policy | 14 |
| 5. Breach Notification..... | 16 |
| 6. Privacy Training | 16 |
| 7. Exemptions and Special situations..... | 17 |
| 8. Reports | 18 |
| 9. Rules and Consequences Policy..... | 18 |
| Chapter 4. Personnel Records | |
| 1. Purpose and Scope | 20 |
| 2. Safeguarding Personnel Records | 20 |
| 3. Electronic Official Personnel Folder (eOPF)..... | 20 |
| 4. Record Keeping Standards..... | 20 |
| 5. FAA Privacy Officer/Privacy Coordinators..... | 20 |
| 6. OPM/GOVT System Notices..... | 21 |
| 7. Conditions of Disclosure..... | 21 |
| 8. Accounting of Disclosures..... | 23 |
| 9. Disclosures within the FAA..... | 23 |
| 10. Access to and Correction of Personnel Records and Privacy Act Inquiries | 23 |
| 11. Request for Access..... | 23 |
| 12. Denial of Access | 25 |
| 13. Request for Amendment or Correction to Personnel Records..... | 26 |
| 14. FAA Initiated Amendment or Correction to Personnel Records | 27 |
| 15. Privacy Act Inquiries | 27 |
| 16. Standards of Accuracy for Personnel Records..... | 27 |
| 17. Specific Personnel Records..... | 28 |

| <i>Paragraph</i> | <i>Page</i> |
|--|-------------|
| Chapter 4. Personnel Records (Continued) | |
| 18. Fees. | 28 |
| 19. Federal Personnel Payroll System (FPPS)..... | 28 |
| Appendix A. Acronyms and Definitions | A-1 |
| Appendix B. Personnel Records Management Guidance for Managers..... | B-1 |
| Appendix C. Privacy Records Management Processes and Procedures Guidance | C-1 |
| Appendix D. Guidance for Chapter 3.2, Disclosure and Access to Records..... | D-1 |
| Appendix E. Reporting Incidents | E-1 |
| Appendix F. Security Controls for Protection of PII | F-1 |
| Appendix G. Information System Security Plan for Records Systems | G-1 |
| Appendix H. Privacy Impact Assessment (PIA) Template | H-1 |
| Appendix I. Privacy Threshold Analysis(PTA) Template..... | I-1 |
| Appendix J. References | J-1 |
| Appendix K. FAA Form 1320-19, Directive Feedback Information..... | K-1 |

Chapter 1. General Information

1. Purpose of this Order.

a. This order implements within the Federal Aviation Administration (FAA) the Privacy Act of 1974 (the Privacy Act), 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 Department of Transportation (DOT), 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 Privacy Act. It implements the provisions of DOT H 1350.2, Departmental Information Resources Management Manual (DIRMM).

b. The objective of this order, in its format and content, is to provide a single reference source for the protection of personally identifiable information (PII) and privacy records within the FAA.

2. Who This Order Affects. This order applies to all FAA employees, contract personnel, and others who have authorized access to FAA information resources. "Others" include grantees, consultants, licensees, and any person or entity, domestic or foreign, having a formal agreement with the FAA.

3. Where Can I find This Order? You can find this order on the Directives Management System (DMS) website: https://employees.faa.gov/tools_resources/order_notices/.

4. What This Order Cancels. FAA Order 1280.1A, Protecting Privacy of Information about Individuals, dated October 7, 1994, is cancelled.

5. Explanation of Policy Changes.

a. Changes existing roles and establishes new roles and responsibilities;

b. Includes provisions for the E-Government Act of 2002 (Public Law 107-347), the Federal Information Security Management Act (FISMA), DOT privacy regulations, OMB mandates, and other DOT and FAA privacy and records management procedures and guidance;

c. Provides a single reference source that incorporates all FAA higher level policy guidance for the protection of PII and privacy records within the FAA;

d. Amends the record keeping requirements for privacy records management; and

e. Incorporates requirements for both electronic and hard media records.

6. Scope. This order applies to:

a. Any FAA information and information systems that collect, store, process, disseminate, transmit, or dispose of information, or those information systems managed by contract personnel for the FAA, and non-FAA owned information systems that access FAA information or information systems. An information system can be either electronic (e.g., computers, PDA's,

hard drives, CDs/DVDs thumb drives, or other multi-media devices.), paper (e.g., reports, records, files, phone books, etc.), or plastic (e.g., microfiche, tapes, etc.), or any other media.

b. Systems include but are not limited to the National Airspace System (NAS), mission support systems, administrative information systems, any information system funded by the FAA, all information systems connected to FAA information or information systems, and prototype information systems connected to any FAA operational and non operational information and information systems.

7. Background.

a. The legislative imperatives for managing privacy information is the Privacy Act of 1974 [5 United States Code (U.S.C.) § 552a as amended], the E-Government Act of 2002, FISMA, and the Homeland Security Act 2002 (Public Law 107–296).

b. Advances in technology and increased reliance on digital data systems, especially in the performance of government affairs, have greatly complicated the challenge of managing privacy information in recent years. Accordingly, a great deal of policy guidance has been provided to assist in meeting this challenge. A summary of the more important policies on managing privacy information is provided in Appendix J of this Order.

Chapter 2. Roles and Responsibilities

1. Roles and Responsibilities.

a. FAA Privacy Officer. The FAA Privacy Officer is responsible for administering the provisions of the FAA Order on Protecting Personally Identifiable Information (the Privacy Order). The Privacy Officer must be a fulltime Federal employee and occupy a high risk information resources position in accordance with the FAA Order 1600.1, Personnel Security Program. Responsibilities include but are not limited to:

- (1) Train employees on the Privacy Act and associated orders, regulations, and OMB guidance;
- (2) Provide guidance on the collection, reporting, and maintenance of data;
- (3) Act as the FAA privacy liaison for all FAA Lines of Business (LOB)/Staff Offices (SO) and work with LOB/SO management to assign Privacy Coordinators;
- (4) Act as the FAA liaison to the DOT Privacy Officer;
- (5) Follow DOT 49 Code of Federal Regulations (CFR) part 10, Maintenance of and Access to Records Pertaining to Individuals;
- (6) Ensure appropriate privacy protections exist for PII that are collected, stored, disseminated, transmitted, or disposed of by information systems owned or operated by or for the FAA,
- (7) Identify and address privacy implications of legislative and regulatory proposals affecting the FAA;
- (8) Conduct periodic reviews of FAA privacy procedures and safeguards for compliance with federal standards;
- (9) Develop an agency process for the completion, review and approval of System of Records Notices (SORNs), Privacy Threshold Analysis (PTAs), and Privacy Impact Assessments (PIAs);
- (10) Develop SORNs for all Privacy Act systems in the FAA system inventory;
- (11) Review and approve all PTAs, via the Privacy Threshold Review (PTR) (which is the last page of the PTA);
- (12) Review and approve all PIAs;
- (13) Ensure adequate resources and staff are devoted to meeting the FAA privacy-related functions and obligations;
- (14) Develop appropriate notifications regarding the agency's privacy policies and privacy-related inquiries and compliance procedures;

(15) Generate privacy-related reports from the FAA to the DOT Inspector General, Congress, or the President;

(16) Report annually or as needed to the FAA Administrator and the DOT Chief Information Officer (CIO) on the effectiveness of the agency privacy program, including progress of remedial actions;

(17) Develop, issue, and maintain agency-wide privacy policies, standards, requirements, guidelines, and procedures in support of this policy;

(18) Implement control measures for paper and electronic systems of records;

(19) Serve as the privacy liaison to the DOT, DOT Inspector General, Congress, and other external organizations;

(20) Review external policies, alerts, guidance, and technical standards and advise LOBs and SOs of major changes that impact the FAA privacy program;

(21) Ensure compliance with all privacy requirements in this order and imposed on the FAA under Federal laws, policies, standards, regulations, and guidelines:

(a) Establish, document, publish, and manage a process for conducting privacy compliance reviews, including but not limited to annual PTAs, PIAs, and periodic system and organization privacy process implementation reviews, in collaboration with the Privacy Coordinators, and ISSMs;

(b) Advise senior agency officials on proper procedural, contractual, technical, or programmatic actions to correct privacy-related deficiencies;

(c) Ensure regular and systematic assessment of the FAA privacy program through a combination of self assessments, independent assessments and audits, formal testing and certification; and

(22) Conduct annual privacy training for FAA employees and contractors.

(23) Serve as the principle advocate for former and current FAA personnel whose personally identifiable information has been compromised, disclosed or released to unauthorized persons.

b. Assistant Administrator for Information Services (AIO-1) and Chief Information Officer (CIO). AIO-1 is the agency focal point and has overall responsibility to oversee the protection of agency PII and information systems including all Privacy Act Systems of Records. The FAA CIO must:

(1) Issue implementation directives, provide interpretation and guidance regarding this order and the FAA Privacy Program;

(2) Consolidate and develop agency responses to privacy inquiries received from Congress, OMB, Government Accountability Officer (GAO), DOT, and other organizations;

- (3) Recommend and approve encryption protection for use on mobile storage devices that carry PII data;
- (4) Manage privacy breach notification policy within the FAA;
- (5) Make final FAA appeal decisions or delegates the decision to a designated FAA employee; the decision is made after consultation with the Chief Counsel; and
- (6) Serve as or designate a co-chair to the FAA Data Governance Board (FDGB) responsible for reviewing Privacy Act computer matching programs.

c. Authorizing Official (AO). In coordination with the FAA Privacy Officer, the AO is accountable for operating a system at an acceptable level of privacy risk for the LOB to agency operations, agency assets, or individuals. In determining acceptable privacy risk, the AO must ensure that their organization identifies all systems under his or her control and completes all privacy-related efforts successfully. The AO must:

- (1) Accept the privacy risk in systems within the AO's purview;
- (2) Assure that the privacy risk is remediated to an acceptable level;
- (3) Order the removal of PII from systems upon which the privacy risk cannot be reduced to an acceptable level, or;
- (4) In cases where it is not possible or economically feasible to remove PII from a system, order operational suspension of systems upon which privacy risk cannot be reduced to an acceptable level.

d. Chief Information Security Officer (CISO). The FAA Chief Information Security Officer (CISO) will provide input to the FAA CIO and FAA Privacy Officer on the effectiveness of the agency wide privacy program.

e. Office of the Chief Counsel (AGC). The AGC is responsible for providing assistance to the CIO and FAA Privacy Officer with respect to the resolution within FAA of all legal matters relating to the Privacy Act, including interpretations of the letter and spirit of the Privacy Act, drafting legal documents necessary to implement the Privacy Act, and coordinating with the General Counsel in the DOT Office of the Secretary of Transportation (OST). AGC is responsible for making all final determinations to deny access or to amend records. Concerning data integrity and data management matters, the Designated Data Authority (DDA) for the AGC is a named participant on the FAA Data Governance Board (FDGB).

f. Regional and Center Assistant Chief Counsels. Regional and Center Assistant Chief Counsels are responsible for providing legal assistance to the offices within their jurisdiction.

g. Assistant Administrator for Security and Hazardous Materials (ASH-1). ASH-1 establishes security standards and safeguards for protection of classified national security information, including classified national security systems, and controlled/sensitive unclassified information within the FAA. ASH-1 is also the Authorizing Official for classified national security systems. The FAA prescribed standards for handling, safeguarding, transmitting and

disposing classified and sensitive unclassified information and materials. These standards are published in FAA Orders 1600.2 and 1600.75. ASH-1 also:

- (1) Provides assistance to FAA organizations on security policies, processes and procedures regarding requests for release or disclosure of classified and sensitive unclassified information; and
- (2) Audits and monitors protection of privacy information and records in connection with Servicing Security Element (SSE) security oversight functions; (ASH-1 will share responsibility with AIO-1); and
- (3) Investigates alleged or actual FAA PII violations. ASH will involve additional LOB/SO personnel in the investigation when appropriate.

h. Regional Administrators. In accordance with FAA Order 1100.154A, paragraph 7.L, regional administrators have signatory authority for administrative matters that 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.

i. Information Stewards. Information Stewards, including designated individuals with CIO responsibilities within the specific line of business/staff office (LOB/SO). Information Stewards and personnel with CIO responsibilities within the LOB/SO must:

- (1) Report when revisions are needed in the systems of records under their control in a manner consistent with the letter and spirit of the FAA Privacy Order. These responsibilities include, but are not limited to, the following specific activities, and are performed by the Information Steward along with the Privacy Officer;
- (2) Limit systems of record PII access to authorized personnel and contractors;
- (3) Receive and process requests for FAA records from persons to whom the records pertain, and ensure the proper identity of requesters and their entitlement to the requested information: Information Stewards must:
 - (a) Receive and process requests from individuals to amend records pertaining to them;
 - (b) Provide facilities and services for inspecting and copying records;
 - (c) Collect fees and charges for copying and certifying records in accordance with 49 CFR Part 10 of DOT Regulations;
 - (d) Prepare required reports concerning the system(s) of records;
 - (e) Review the published Privacy Act system notice for accuracy and initiate action to update the notice due to changes in information and information systems.
 - (f) Regularly inspect for compliance and enforce rules of system use for all employees who have access to privacy information and systems that contain privacy information;

(g) Distribute this policy and related procedures to all employees and contractors that have access to privacy information and systems that contain privacy information ;

(4) Complete or update annually a system PTA for each LOB/SO system identified on the FAA system inventory, and include it in the annual Security Certification and Accreditation Package C&A (Certification and Accreditation).

(5) Complete or update annually a system PIA as required by the system PTA/Privacy Threshold Review (PTR), submit it for review and approval by the FAA Privacy Officer, and include it in the annual C&A/Annual Security Assessment submission.

(6) Use the checklist in Appendix F to evaluate the privacy controls implemented on FAA information and information systems.

(7) Complete for each system in the FAA system inventory the considerations enumerated in Chapter 3, in the section entitled, Collection and Maintenance of Systems of Records.

(8) Document in each system Information System Security Plan (ISSP) the protection of PII.

(9) Include in system budget documentation all system privacy risk remediation activities, identify all remediation activities in the system Plan of Action and Milestones (POAM), and implement planned remediation in a timely manner. Documentation related to this requirement includes but is not limited to:

(a) Remediation time and cost (POAM); and

(b) Budget documentation (funding requests and, when applicable, OMB Exhibit 300).

(10) Document residual system privacy risk in the system C&A.

(11) Perform the following related to Privacy Act systems of records disclosure and access: (see Chapter 3 section entitled "Disclosure and Access to Records")

(a) Grant individuals access to their FAA records;

(b) Deny individuals access to their FAA records or portion thereof when a Privacy Act exemption applies, or when those records were compiled in reasonable anticipation of a civil action or proceeding;

(c) Amend individuals' FAA records when their Privacy Act amendment request is substantiated;

(d) Permit disclosure of records, if authorized under the provisions of Appendix B, Personnel Records Management;

(e) Prior to completing a determination to deny an individual access to or right to amend his/her records, the Information Steward must coordinate the decision with the appropriate Privacy 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.;

(f) If the Information Steward(s), which includes the LOB/SO CIO, Business Owner, and System Owners/Data Steward, is below the division level or equivalent, the manager at the division level or above will, after consultation with legal counsel, make the final determination for disclosure and access to Privacy Act Systems of Records. At the aeronautical center, the records coordinator maintains program oversight at the directorate level. A determination for access or denial to records is made at the directorate level.

(g) Initiate cancellation of existing FAA systems of records by documenting rationale supporting cancellation, identifying the recommended cancellation date and forward the documentation for FAA Privacy Officer review and approval.

(h) Maintain a log of individuals who request access to or request amendment of records about themselves that are contained in the systems of records.

j. Information System Security Manager (ISSM). All FAA ISSMs must comply with the roles and responsibilities prescribed in FAA Order 1370.82A and carry out the following responsibilities:

(1) Serve as the principal adviser to the AO, CISO, and Information System Owner (ISO) on all matters involving the privacy of the information system, including ensuring privacy policies are disseminated, where applicable, and serve as advisor on privacy-related matters to the FAA Privacy Officer;

(2) Develop Information System Security Plans.

(a) Ensure that each system C&A package contains the required documents, including ISSP, PTA/PTR, and PIA;

(b) Provide privacy policy guidance to the ISSM(s), Information System Security Officers (ISSOs), and other LOB or SO personnel in the performance of their ISS/privacy activities;

(c) Coordinate with management and other key privacy personnel, as appropriate, on various security related matters, including security management, enterprise architecture, and privacy;

(d) Participate in privacy compliance reviews and vulnerability and threat assessments;

(e) Ensure the risk of privacy systems under their purview is identified and remediation is prioritized;

(f) Coordinate with the FAA Privacy Officer when a system configuration change or change in ownership impacts a systems privacy impact assessment;

(g) Assist the Cyber Security Management Center (CSMC) in conducting inquiries into privacy incidents that occur in their area of responsibility, including contacting external

groups and other organizations to better understand the threat posed by incidents, sharing information about incidents, and developing recommendations for LOB or SO management on the best course of action in dealing with incidents; and reporting any privacy violations.

(h) Ensure compliance with Federal mandates and guidelines, including training, resources, funding, distribution of privacy alerts or bulletins, identification of key personnel, and other elements of privacy implementation; and

(i) Oversee the development, implementation, and reporting of privacy mitigation efforts in response to privacy alerts, bulletins, or security and privacy assessments and audits.

k. Privacy Managers. The Privacy Managers must be designated in writing by their respective LOB/SOs and listed on the Privacy Website. Privacy Managers must ensure the responsibilities listed below are complete.

(1) Privacy Managers shall ensure the implementation of and compliance with the FAA Privacy Order within their respective LOB/SO.

(2) Maintain a current file of Privacy Act system notices that impact their respective LOB/SO.

(3) Partner with the Privacy Division on privacy training and awareness activities to ensure that employees know their roles and responsibilities to guarantee that personal data is properly handled.

(4) Oversee privacy support personnel as needed; provide staff advice and assistance within respective LOB/SO to inquiries regarding systems of records, delegated authorities, FAA privacy procedures and privacy controls.

(5) Comply with requests from the FAA Privacy Officer for information and data.

(6) Submit information to the FAA Privacy Officer on all new use or intended use of the PII data and information in a system of records.

(7) Comply with DOT Regulations 49 CFR part 10 (Maintenance of and Access to Records Pertaining to Individuals).

(8) Collaborate with the Privacy Division, ISSM, FOIA staff, records officers, CSMC and ASH/AIN on an as needed or required basis regarding any privacy issues.

(9) Coordinate Flight Plan progress with LOB Business Planner to meet target goals. Manage specific LOB privacy budget, implementation plan and business plan.

(10) Serve as the LOB/SO privacy partner for policy and governance compliance.

(a) Serve as LOB/SO POC for privacy compliance reviews, in accordance with this Order.

(b) Abide by data governance policies to ensure proper considerations of PII usage.

(c) Consistently participate and contribute in privacy governing committees such as the Privacy Working Group.

(11) Manage daily LOB/SO privacy operations

(a) Be accountable for addressing privacy issues in the specific LOB/SOs System Development Lifecycle.

(b) Ensure that PIA/PTAs are generated and updated when necessary.

(c) Responsible for all activities associated with LOB/SOs System of Records Notices.

(d) Ensure development of privacy artifacts required as a part of system authorization, i.e. SORNs, PTA/PIAs.

(e) Serve as the LOB/SO POC for data calls in support of FISMA reporting, Data Loss Prevention activities and incident response for privacy breaches.

l. Cyber Security Management Center (CSMC). The FAA CSMC is responsible for the management and oversight of cyber security and PII incidents for the DOT.

(1) Receive reports of PII incidents and exposures from LOBs and SOs, as they are discovered.

(2) Report PII incidents to the US-CERT, Agency and Departmental Senior Management within one hour of notification.

(3) Receive updates regarding PII incidents from LOBs and SOs.

(4) Receive PII incident resolution reports from the FAA Privacy Officer.

(5) Report resolved PII incidents to US-CERT.

(6) Communicate with ASH, the FAA Privacy Officer and other FAA and DOT personnel on alleged or actual PII incidents.

m. All FAA officials and employees. All FAA officials and employees having agency responsibilities for collecting, maintaining, using, or disseminating records that contain PII are responsible for complying with the provisions of this Order.

2. Other Roles and Responsibilities

a. Department of Transportation Data Integrity Board. The DOT Data Integrity Board was established in compliance with the Computer Matching and Privacy

Protection Act of 1988. This board reviews and approves or disapproves computer matching programs if DOT is either a source or recipient (or matching) agency.

b. FAA Data Governance Board (FDGB). The FDGB reviews all computer matching programs the FAA proposes to conduct with other agencies or state or local governments. This board reviews computer matching programs before the proposed programs are brought before the DOT Data Integrity Board. The FDGB was established by FAA Order 1375.1 (Data Management) and is co-chaired by the agency CIO (AIO-1) or designee, Chief Operating Officer, Air Traffic Organization (ATO-1) or designee, and the Associate Administrator for Aviation Safety (AVS-1) or designee. The manager of the Information Management Division (ARD-300) within AIO acts as the executive secretary.

3. Delegation of Authority.

a. Authority to Change, Revise, or Cancel Directives. The person at the management level who approved the original directive approves changes and revisions, or cancels a directive. Signature authority may be delegated, but only one level lower. This applies, however, only if the new version does not:

- (1) Modify FAA policy;
- (2) Change delegation of authority or assignment of responsibility; or
- (3) Have a significant impact on the resource requirements or level of service provided.

b. Authority to Change Appendices. The Privacy Officer carries the responsibility for recommending changes to this order and its appendices. The Office of Primary Responsibility may cancel and replace procedural appendix changes that are essential to administer functions pertaining to the roles and responsibilities defined in this Order. This applies only to procedural appendices, not policy. Updates to procedural appendices are administrative in nature; therefore, no coordination is required.

c. Guidance for delegation of Authority: For more information concerning FAA Directives Management see Order 1320.1E.

Chapter 3. Policy

1. Requirements.

a. Public law, executive orders, OMB memoranda and guidance, Federal Information Processing Standards (FIPS) publications, National Institute of Standards and Technology (NIST) Special Publications (SPs), DOT policy and guidance, and FAA orders must be followed to properly secure PII.

b. Privacy Act information in a system of records will not be disclosed to any person or to another agency except with the prior written consent of the individual to whom the record pertains. Exceptions are specifically listed in 5 U.S.C. 552a (b) and are detailed in Appendix C, Privacy Records Management.

c. All information collections or information systems must complete or update a PTA annually, using the PTA template provided as an appendix to this Order, and submit it with the C&A documentation for AO review and approval. The PTAs are not considered “approved” until the Privacy Officer completes and signs the PTR, which is the last page of the PTA.

d. If a system’s PTA/PTR determines that a PIA is required, the PIA must be completed/updated and submitted with the C&A documentation for AO review and approval.

e. All Privacy sensitive systems must document in their ISSP the protection of PII.

f. When Privacy sensitive system’s vulnerabilities/risks are discovered, the risk must be remediated to an acceptable level. If it is either impractical or unfeasible to remediate the privacy risk, the PII must be removed from the system or the system’s operation must be suspended.

g. An individual may request amendments to his/her Privacy sensitive records if the individual believes the information is not accurate, relevant, timely, or complete. An individual will be permitted to review and have a copy of all or any portion of FAA Privacy sensitive records that pertain to him/her except for:

(1) Those records compiled in reasonable anticipation of a civil action or proceeding;
or

(2) Those records exempted from the access requirements of the Privacy Act and published as general or special exemptions (see section 7 of this chapter).

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

i. Requests for personal information maintained in an FAA Privacy sensitive system must be made to the FAA Privacy Officer or LOB/SO Privacy Coordinator. All requests by individuals to review or copy his/her 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.

j. 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 manual, automated, and electronic record systems on FAA and non-FAA owned systems. The objective of these controls is to ensure that PII is protected to include confidentiality, integrity, and availability of personal information held by all FAA components.

k. Individuals from whom personal information is requested in connection with FAA programs will be told at the time of the request:

- (1) The authority which authorizes the solicitation of the information;
- (2) Whether providing such information is mandatory or voluntary;
- (3) The principal purposes for which the information is intended to be used;
- (4) The routine uses that may be made of the information; and
- (5) The effects, if any, of not providing all or any part of the requested information.

Note: 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.

l. 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). Exception: The disclosure of the SSN is required by Federal statute if such disclosure was required under statute or regulation adopted prior to January 1, 1975, to verify the identity of the individual.

m. Other existing FAA orders and notices containing specific criteria for obtaining or disseminating information about individuals must be followed so long as the provisions of the Privacy Act as described herein are not violated. Any inconsistencies must be brought to the attention of the FAA Privacy Officer.

2. Disclosure and Access to Records.

a. The Privacy Act's requirements on disclosure of records are stated in Appendix C of this Order. 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, certain disclosures are allowed without the individual's prior written consent as set out in Appendix C. This paragraph pertains to disclosure of records other than personnel records.

b. An individual can gain access to his/her record or to any information pertaining to him/her that is contained in a system of records. Follow the procedures in Appendix C.

c. When a record is requested that is contained in a system of records maintained by the FAA, but which originated in another Federal agency, follow the procedures in Appendix C.

3. Collection and Maintenance of Systems of Records. 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 improper use of personal data, whether intentional or inadvertent. It is therefore incumbent on the FAA to review existing practices pertaining to the collection and disclosure of PII. The following considerations must be evaluated by all Information Stewards regarding PII or reviewing and maintaining PII collected:

- a. Determine if collection is necessary by performing a PTA;
- b. Ensure that all collections must relate to the principal purpose for which the information is maintained;
- c. Ensure that all collections must state the consequences, if any, of not collecting that information;
- d. Confirm whether or not a sampling procedure would suffice in collecting information;
- e. Determine the point at which information collected will satisfy the purpose for which it is collected. In addition, it is important to know how long it is necessary to retain the information;
- f. Determine the costs/benefits of maintaining PII in the system or removing it from the system;
- g. Determine whether each item of information is absolutely essential;
- h. Determine what security measures will be required and what these measures cost.

Note: These considerations are not all-inclusive nor are they applicable to all systems of records. However, where applicable, each should be considered. The FAA is subject to requirements of the Computer Matching and Privacy Protection Act of 1988 and the Computer Matching and Privacy Protection Amendments of 1990. For certain types of computerized matching programs (typically across two or more computer programs), the FAA must follow requirements for written agreements for such matching programs, a review and approval process through the DOT Data Integrity Board, procedures for due process and annual reviews, and other related procedures.

4. Safeguarding Policy.

- a. **The Privacy Act.** The FAA must have:

(1) Appropriate management, operational, and technical controls to ensure the confidentiality, integrity, and availability of Privacy Act records. A listing of the public law, executive orders, policies, directives and guidance pertaining to these controls and privacy in general is available in Appendix J of this Order. Other references not specifically identified in Appendix J may also apply.

(2) Rules of behavior for individuals involved in the design, development, operation, or maintenance of any system of records, or for individuals maintaining any PII; and

(3) Instructions for individuals about such rules and the requirements of the Privacy Act and its implementing rules and procedures, and the penalties for noncompliance.

b. Reduce Volume of PII. Information Stewards must reduce the volume of PII in their records to the minimum necessary to conduct business and dispose of the records, per FAA Order 1350.14A, and 1350.15C Records Management, when those records are no longer needed. By collecting only necessary information and disposing of unnecessary information, we reduce the volume of information we hold, the risk to the information, and the cost of safeguarding it.

c. Eliminate the Unnecessary Use of Social Security Numbers (SSN) in Privacy Sensitive Systems. Information Stewards must not:

(1) Use SSNs as a data element in a record unless a law or directive requires its use or the FAA Privacy Officer approves its use; and

(2) Use an SSN, or any part of an SSN, as a personal identifier. Personal identifiers are data elements that identify a unique individual and can permit another person to assume that individual's identity without their knowledge or consent.

d. Complete Background Investigations for Persons Who Have Access to Privacy Sensitive Systems. Before an FAA employee or contractor may have access to PII systems, the employee or contractor must undergo a background investigation consistent with Homeland Security Presidential Directive 12 (HSPD 12).

e. Assign Impact Levels to PII Information and Information Systems. In accordance with Federal Information Processing Standard 199 (FIPS 199) agencies must set up standards for categorizing information and information systems. Per FIPS 199, PII falls under the privacy security category.

(1) When FAA records contain PII, information stewards must assign at least a moderate impact level to the information; and

(2) When FAA records contain PII, information stewards must assign a moderate or high impact level to the information and information system.

f. Control Access. Access to PII must be limited to authorized personnel and contractors. see Appendix D of this Order for additional guidance concerning access. (also see the privacy website, <http://www.faa.gov/privacy/>)

g. Store PII on Government Systems Only. DOT policy only allows the downloading and storage of PII on FAA-owned equipment or systems and authorized support contractor systems. Storage of PII on unauthorized non-FAA-owned equipment and mobile devices is prohibited.

h. Encrypt PII on Mobile Computers and Devices. PII data stored or carried on a FAA-owned mobile computer or FAA-owned storage device must be encrypted using the FAA CIO-approved and recommended encryption.

i. Select Suitable Security Controls For Electronic Record Systems. Privacy Sensitive Systems security control standards are selected based on the guidance provided in FIPS 200,

Minimum Security Requirements for Federal Information and Information Systems. These Electronic Records System must be in a suitable environment in which limited authorized access occurs considering the nature and volume of information. Systems must have administrative, technical, physical, personnel, and security controls for both electronic and paper records.

j. Select Suitable Security Controls for Manual or Paper Record Systems. Security controls for manual or paper systems of records must be selected from those published by the FAA Privacy Officer. See Appendix F.

5. Breach Notification. Incidents of possible or confirmed PII theft, loss, or unauthorized disclosure, and suspected or actual loss of PII control must be reported immediately in accordance with DOT/FAA security incident reporting and response policy and guidance. Lack of complete information must not prevent reporting of incidents in which PII may have been compromised.

a. All real or suspected incidents in which PII may have been compromised must be reported immediately upon discovery to the CSMC. The CSMC will notify US-CERT, FAA Privacy Officer and other Agency and Departmental Senior Management.

(1) Information Stewards. Information Stewards are normally the first people to find out about an incident of possible or confirmed compromise of PII. They must make an initial report of any incident to their ISSM, LOB or SO management and to their SSE within an hour of finding out about an incident. Appendix E has guidance for collecting facts about an incident. Incomplete facts must not delay the initial report. Specific incidents will likely create more questions and may require a thorough inquiry and even a formal investigation;

(2) LOB, SO, or SSE Management. In addition to reporting incidents to the CSMC, and depending on their reporting chain, LOB, SO, or SSE management must also report incidents to their Regional Operations Center (ROC) or National Operations Command Center (NOCC) within an hour of finding out about the incident.

(3) ROC or NOCC. Depending on their reporting chain, the ROC or NOCC reports the incident to the Washington Operations Center (WOC) or the CSMC.

(4) WOC or CSMC. The WOC notifies the CSMC or the CSMC notifies the WOC; and

(5) WOC. The WOC then notifies the ASH-1, DOT, Domestic Events Network, and the Security Information Group.

b. After informing the CSMC, the Privacy Officer in conjunction with appropriate agency personnel will provide an assessment of impact on the FAA and the individuals whose personal information has been put at risk.

6. Privacy Training. All FAA employees and contractors must receive privacy training annually to ensure that all employees and contractors understand their responsibility for protecting information in identifiable form. Privacy training includes the duties under Section 208 of the E-Government Act, the Privacy Act, and other privacy laws and policies. Training

must remind employees of their responsibility for safeguarding PII, the rules for acquiring and using such information, and the penalties for violating these rules. In addition, the Privacy Officer provides training on an “as needed” basis.

7. Exemptions and Special Situations.

a. General Exemptions. The Privacy Act permits the head of an agency to publish rules exempting any system of records from certain provisions of the Privacy Act if the system of records is maintained by an agency or a component agency that 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.

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

(1) Material required to be kept classified by Executive Order in the interest of national defense or foreign policy;

(2) 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 must 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;

(3) Records maintained in connection with providing protective services to the President of the United States or other individuals pursuant to section 356 of U.S.C. Title 18;

(4) Records required by statute to be maintained and used solely as statistical records;

(5) 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;

(6) 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; and

(7) 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.

8. Reports.

a. New or Revised Privacy Sensitive Systems . A report must be submitted to the FAA Privacy Officer for each new system of records and for changes to existing systems. The report can be submitted during the information system security annual Certification and Accreditation (C&A). The FAA Privacy Officer must publish a systems of record notice in the Federal Register or a Privacy Impact Assessment. The criteria for determining what constitutes a change to an existing system requiring the preparation of a notice or PIA 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 personally identifiable 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 purpose 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; or

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

b. Privacy Act Statistical Summary. Statistical summaries and reports must be completed and submitted consistent with public law, and OMB policy/guidance.

c. FISMA Report. FAA participates in the quarterly and annual departmental reports.

d. E-Government Report. The FAA participates in the annual departmental e-Government Report under the provisions of FAA Order 1370.82, Information System Security Program.

e. Consolidated Appropriations Act of 2005 Section 522a for Transportation, Treasury, and Others Agencies Report. The FAA participates in the annual departmental consolidated report.

9. Rules and Consequences Policy.

a. Ensure that managers and employees are informed and trained regarding their respective responsibilities relative to safeguarding PII and the consequences and accountability for violation of these responsibilities. Therefore, it is the responsibility of each agency to develop and implement an appropriate policy outlining the rules of behavior and identifying consequences and corrective actions available for failure to follow these rules. Consequences should be commensurate with the level of responsibility and type of PII involved. Managers must also be reminded of their responsibility to instruct, train, and supervise employees on safeguarding PII. See Appendix C of this Order.

b. Rules of System Use. The corrective actions must:

(1) Describe the user's responsibilities and expected behavior with regard to information and information systems usage. The rules of system use must notify the user of PII information/data contained within the information system, when applicable.

(2) The user must sign (written or electronic signature) an acknowledgement indicating they have read, understand, and agreed to abide by the rules of system use, before obtaining access to the information and information system.

(3) The rules of system use must comply with minimum requirements specified in NIST SP 800-18, DOT and FAA information system security policy.

c. Consequences. Consequences may include reprimand, suspension, removal, or other actions in accordance with applicable law and agency policy. The minimum consequence agencies must consider is prompt removal of authority to access information or systems from individuals who demonstrate egregious disregard or a pattern of error in safeguarding PII.

Chapter 4. Personnel Records

1. Purpose and Scope. This chapter sets forth basic policies governing the creation, development, maintenance, processing, use, dissemination, and safeguarding of personnel records that the OPM requires the FAA to maintain in the personnel management policy consistent with 5 CFR 293. It also sets forth the regulations to govern the maintenance, protection, disclosure, and amendment of records within the system of records as defined by the Privacy Act of 1974 and 5 CFR 297. As a result of FAA Reform in 1996, while the FAA is not specifically covered, for this Order we adopted provisions in 5 CFR 293, 294, and 297. Title 5 CFR 297.104 covers three generic types of personnel records systems. See AHR policy division for specific HR standardized documents. The three generic types of personnel records systems are internal systems, centralized systems and government wide systems.

2. Safeguarding Personnel Records. The OPM requires Federal Human Resource officials to create, maintain, and safeguard employee information in accordance with the Privacy Act of 1974 (5 U.S.C. 552a). This requirement has been delegated to Federal agencies, including the FAA. These requirements mandate the maintenance and safeguarding of the consolidated system of records on employees, including the Official Personnel Folder (OPFs) and employment-related files. Duplicating and maintaining copies of SF-50s and OPFs are direct violations of the delegated system of records requirements. A person who discloses personally identifiable information (PII) from personnel records subject to the Privacy Act, knowing that the disclosure is unauthorized, may be subject to disciplinary action up to and including removal from Federal service, as well as criminal sanctions.

3. Electronic Official Personnel Folder (eOPF). The FAA migrated to eOPF in March 2008. Migration to eOPF means access to the OPF will be limited to the Human Resource Management offices. Time-limited access may be given to others (i.e., managers and OPM approved investigators, etc.), on a “need to know” basis when the data is legitimately needed. Initiating a personnel action does not constitute a “need to know”. Individual employees will have access to their own official personnel files with the capacity to review and print documents from his/her own folder. The electronic version will be the “official” personnel file. The original paper OPFs will no longer be maintained and are forwarded to the National Archives and Records Administration (NARA). Upon separation from the Federal service, electronic files will be forwarded to the NARA for appropriate disposition according to OPM’s rules and regulations.

4. Record Keeping Standards. The administrator must ensure that persons having access to or involved in the creation, development, processing, use, or maintenance of personnel records are informed of pertinent recordkeeping regulations and requirements. Information in the personnel record will contain only information concerning the individual that is relevant and necessary to accomplish the Federal personnel management purposes required by statute, Executive order, or office regulation.

5. FAA Privacy Officer (Chapter 2.1.a.)/Privacy Coordinators (Chapter 2.1.k.) responsibilities. The Privacy Officer and Coordinators are responsible for assisting Human Resource Directors in discharging his/her personnel management responsibilities under the Privacy Act. They also ensure human resource employees and FAA managers are made aware of their responsibilities regarding personnel records under the Act. Privacy Coordinators serve as the human resources organization communication channel providing advice and assistance

regarding the personnel implications of the Act. They ensure that personnel orientation programs include a general discussion of individual employee responsibilities under the Privacy Act. The Privacy Coordinator cooperates and refers unresolved problems to the jurisdiction's Regional Assistant Chief Counsel. If further advice is needed, the problem must be referred to the Assistant Administrator for Information Services and Chief Information Officer (FAA CIO). The Office of the Chief Counsel will provide interpretations and legal drafting necessary to implement the Privacy Act.

6. OPM/GOVT (government) System Notices. The OPM/GOVT system notices are published in the Federal Register. (<https://www.opm.gov/feddata/Federalr.txt>)

7. Conditions of Disclosure. Any information in a system of records must not be disclosed to any person or to another agency, or another entity without the express written consent of the subject individual to whom the record pertains. Prior written consent, if obtained, must be specific, not open-ended, stating the general purpose for and names and types of recipients to whom disclosure(s) may be made. Conditions in which disclosures of personnel records may be made without prior written consent are found in Chapter 3.2, Disclosure and Access to Records and Appendix C.1, Disclosure without Prior Written Consent.

a. One of the conditions for which an employee's/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 (FOIA). The following employee information contained in personnel records must be disclosed under FOIA upon request:

- (1) Name;
- (2) Present and past Federal position titles;
- (3) Grades;
- (4) Salaries; and
- (5) Duty stations (which include room numbers, shop designations, or other identifying information regarding buildings or places of employment).

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 Chapter 3.2, Disclosure and Access to Records, and Appendix C.1, Disclosure without Prior Written Consent. For example, disclosures may be made for a routine use that has been established and described in the public notice required by the Privacy 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 FOIA and the request is not accompanied by the employee's prior written consent. The personnel office, as an alternative to 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 addresses the eOPF, 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 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) The parent of any minor; or

(2) The legal guardian of any individual who has been declared to be incompetent due to physical or mental incapacity or age by a court of competent jurisdiction, and may act on behalf of the individual under 5 U.S.C., section 552a (h) and in accordance with the applicable section of 5 CFR 297.

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 Appendix C.3, Access to Records, and C.4, Handling Requests for Records and Corrections, for additional provisions regarding medical records only.

e. Special procedures regarding disclosures of certain personnel records in response to congressional inquiries only. 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 discussed below.

(1) 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 that they request.

(2) 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:

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

(b) 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) 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 human resource office will advise the congressional office that written consent is required. The human resource office should not contact the employee or applicant unless the congressional office requests the human resource office to do so.

(4) The human resource office will respond to any congressional inquiries without disclosing information contained in records subject to the Privacy Act.

(5) 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:

(a) If the information would be required to be disclosed under the FOIA (Chapter 4- 7.a);

(b) If the member requests that the response go directly to the individual to whom the personnel record pertains; or

(c) Under the provisions of Appendix C.1.c, C.1.e (including statistical records), C.1.h, and C.1.i.

8. Accounting of Disclosures. The Privacy Act requires that agencies account for disclosure of records. Further information regarding Accounting of Disclosures is discussed in Part 297 of the OPM regulations. The FAA will maintain a record of disclosures in cases where records about an individual are disclosed from an office system of records except when:

a. Disclosure is pursuant to the FOIA, as amended (5 U.S.C. 552);

b. Disclosure is made to employees of the FAA who have a need for the record in the performance of their duties; or

9. Disclosures within the FAA. When personnel records are disclosed from one organizational unit to another (such as information from an OPF from a human resource office to a manager with a “need to know”) the receiving individual is responsible under the Privacy Act for maintaining them, including any further dissemination.

10. Access to and Correction of Personnel Records and Privacy Act Inquiries. The procedures described in paragraphs 11, 12, and 13 below 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 3 (which relate to all other FAA systems of records). In order to ensure clarity and consistent application of both the FAA and OPM provisions relating to access 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.

11. Request for Access. An employee or applicant must be granted access to personnel records pertaining to him/her upon request. When a request is received, the information steward or designee must:

a. Determine whether the request should be handled under the FOIA or Privacy Act (see Appendix C.3).

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

c. Notify the requester of the following within ten workdays:

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

(a) Inspection, in person, in the office specified by the information steward, during the hours specified;

(b) Transfer of the personnel record to another FAA office, an OPM office, or other Federal facility more convenient to the requester, but only if the information steward 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; or

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

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

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

(4) The period of time the personnel records must 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 11.c.3 above applies) and an estimate of fees when appropriate and pursuant to Appendix C.

(6) If the requester wishes, he/she 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 that are described in paragraph 7a. above.

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 12 below. In no event will original personnel records of the OPM or the FAA be

made available to the individual except under the immediate supervision of the information steward or designee. The U.S.C. Title 18, section 2701, makes it a crime to conceal, mutilate, obliterate, or destroy any record filed in a public office, or attempt to do so.

g. Observe the right of any employee or applicant who requests access to a personnel record pertaining to him/her to be accompanied by another individual of his/her choice. "Accompanied" includes discussion of the record in the presence of the other individual. The person to whom the record pertains must authorize the presence of the other individual in writing and must 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 must sign the authorization in the presence of the information steward or designee. An employee or applicant must not be required to state a reason or otherwise justify his/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.

i. Ensure that the provisions of the Privacy Act are complied with in a timely manner.

j. Deny access in accordance with the Privacy Act System Notices.

k. Annotate such internal records as may be necessary to account for all such disclosures.

12. Denial of Access. Access by an employee or applicant to personnel records pertaining to him/her will be denied *only* upon a determination by the information steward or designee that one or more of the following grounds exist:

a. For Government-wide personnel records:

(1) A personnel record is subject to an exemption under Title 5 CFR Part 297 (Privacy Procedures for Personnel Records).

(2) The provisions of Title 5 CFR Part 297 pertaining to medical records apply;

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

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

b. For FAA-wide personnel records:

(1) The provisions of Title 5 CFR Part 297 or paragraphs pertaining to medical records apply.

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

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

Note: For more information and guidance regarding denial of access, see Appendix C.

13. Request for Amendment 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 FAA. The request must be made in writing to the information steward indicated in system of records notice and state that the request is being made pursuant to the Privacy Act of 1974. (The remainder of this paragraph deals with requests received by the FAA.)

b. 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 must 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.

c. Any request that is not addressed as specified in paragraph 13.a or not marked as specified Privacy Act of 1974 will be so addressed or marked by FAA personnel and forwarded immediately to the responsible information steward. 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 information steward receives it. In each instance when a request so forwarded is received, the information steward or his/her designee must notify the individual that his or her request was improperly addressed and annotate the date when the request was received at the proper address.

d. 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 4.11.b should be utilized. Written request should be submitted to eOPF workgroup administrators at the Shared Service Centers.

e. A request for correction or amendment must 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; and
- (4) A statement of the basis for the requested correction or amendment, with all available supporting documents and materials that substantiate the statement.

f. Not later than ten workdays after receipt of a request to correct or amend a record, the information steward or his/her designee must send an acknowledgment providing an estimate of time within which action will be taken on the request. If a response cannot be made within ten workdays due to unusual circumstances, the information steward must 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 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 and processed, and the individual notified of the results of review (either compliance or denial) within ten 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.

g. After acknowledging receipt of a request and receiving such additional information as might have been requested, the information steward or his/her designee will review and take action. For the process this action will follow, see Appendix C.

h. Correction or amendment of a record will be denied upon a determination by the information steward 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 required to process the request to correct or amend the record; or
- (5) If a request is partially granted and partially denied, the information steward must follow the appropriate procedures of this order as to the records within the grant and the records within the denial.

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.

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

16. Standards of Accuracy for Personnel Records. To minimize the risk that the FAA will make an unwarranted adverse personnel determination or disseminate inaccurate information about an employee or applicant, all personnel records that are used in making any such determination must 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; and
- f. The degree of possibility that the information could unfairly result in an adverse determination.

17. 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 OPF, OPM/GOVT system notices suffice.

b. Merit Promotion Plan (MPP) Records. These records, which the OPM requires to be maintained, are generally filed by announcement number. 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 OPF's is covered by the 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., Resume). The OPM system notices cover applications if they are maintained in an Applicant Supply File. Also covered are applications that are received for a specific vacancy and returned to the applicant. Applications will be maintained in the Merit Promotion File unless a different procedure is specifically authorized by the Administrator.

d. Medical Records. The OPM system notices cover medical data required by OPM. However, medical data contained in health unit records that are subject to the requirements of the Privacy Act are covered by an FAA published system notice. Please see: <http://www.dot.gov/privacy/privacyactnotices/faa.htm>. Alcohol and drug records subject to the Act and referenced to in 5 CFR, chapter 792, are covered by an OPM system notice.

18. Fees. (Fees are found in Appendix C part 10). The guidance for Office of Personnel Management fees is contained in 5 CFR 294. The agency is using eOPF which allows the FAA employee to make their own copies of SF 50's their Notification of Personnel Actions.

19. Federal Personnel Payroll System (FPPS). FPPS is covered by OPM Government wide Systems of Records OPM/GOVT-1 (General Personnel Records) as defined in 5 U.S.C. 2105.

Appendix A. Acronyms and Definitions

Acronyms used in this Order are listed immediately below. A list of definitions of selected acronyms and other terms is included following the list of acronyms.

1. Acronyms:

AES – The Information Technology
Business Enterprise Services
Division

AIO – Assistant Administrator for
Information Services

AIS – Office of Information System
Security

AO – Authorizing Official

ASH-Assistant Administrator for Security
and Hazardous Materials

ATO – The Air Traffic Organization

AVS – The Associate Administrator for
Aviation Safety

C&A – Certification and Accreditation

CFR – Code of Federal Regulations

CIO – Chief Information Officer (AIO-1)

CISO – Chief Information Security Officer

CSMC – Cyber Security Management
Center

DDA – Designated Data Authority

DHS – Department of Homeland Security

DIRMM – Departmental Information
Resources Management Manual

DMS – Directives Management System

DO – Deciding Official

DOT – Department of Transportation

EEO – Equal Employment Opportunity

eLMS – Electronic Learning Management
System

eOPF – Electronic Official Personnel Folder

FAA– Federal Aviation Administration

FAST – FAA Acquisition System Toolset

FDGB – FAA Data Governance Board

FIPS – Federal Information Processing
Standard

FISMA – Federal Information Security
Management Act of 2002

FOIA – Freedom of Information Act

FPPS – Federal Personnel Payroll System

GAO – Government Accountability Office

GDO – Grievance Deciding Official

GFT – Guaranteed Fair Treatment

HRMD –Human Resource Management
Division

ISO – Information System Owner

ISSM – Information System Security
Manager

ISSO – Information System Security Officer

ISSP - Information System Security Plan

IT – Information Technology

LAN – Local Area Network

LOB – Line of Business

NAS – National Airspace System

MPP – Merit Promotion Plan

MSPB – Merit System Protection Board

NARA – National Archives and Records
Administration

NIST – National Institute of Standards & Technology

NDA – Non-Disclosure Agreement

NOCC – National Operational Control Center

NSN – National Stock Number

ODP – Opportunity to Demonstrate Performance

OPF – Official Personnel Folders

OMB – Office of Management and Budget

OPM – Office of Personnel Management

OPR – Office of Primary Responsibility

OST – Office of the Secretary of Transportation

PIA – Privacy Impact Assessment

PII – Personally Identifiable Information

PIV – Personal Identity Verification

PTA – Privacy Threshold Analysis

PTR – Privacy Threshold Review

ROC – Regional Operations Center

SO – Staff Office

SORN – System of Records Notice

SP – Special Publication

SSE – Servicing Security Element

SORN – System of Record Notice

SSN – Social Security Number

SUI – Sensitive Unclassified Information

USB - Universal Serial Bus

U.S.C. – United States Code

US-CERT- United States Computer Emergency Readiness Team

WAN – Wide Area Network

WOC – the Washington Operations Center

2. Definitions:

Access: The ability or opportunity to gain knowledge of PII.

Applicant: An individual who has applied for FAA employment.

Chief Information Officer: A senior level executive charged with information technology (IT) and ISS oversight and financial authority for agency assets and information system under his or her control (e.g. LOB, SO). AIO-1 is the overall agency CIO for FAA

Control: The authority of the government agency that originates information, or its successor in function, to regulate access to the information. Having control is a condition or state and not an event. Loss of control is also a condition or state which may or may not lead to an event, i.e., a breach.

Employee: A current or former FAA employee.

Individual (1): For purposes of the Privacy Act, an individual is a citizen of the United States or an alien lawfully admitted for permanent residence.

Individual (2): For purposes of safeguarding and encrypting PII, an individual is any human being, living or deceased, regardless of nationality.

Information Security: Information security is the system of administrative and technical security directives, rules, policies, procedures and practices for how an organization identifies, manages, controls, protects and distributes information requiring protection as required by Executive Order, law or regulation.

Information: Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics.

Information Steward: As specified in FAA Order 1375.1, as amended, the Information Steward is an agency official with statutory or operational authority for managing specified information and is responsible for establishing the controls for the generation, collection, processing, dissemination, and disposal. The Information Steward may be the same as the ISO.

Office of Primary Responsibility (OPR): That staff or program office which has principal cognizance for policies and procedures over particular areas.

Personally Identifiable Information (PII): Any information about a human being, living or deceased, regardless of nationality, that is maintained by an agency and that permits identification of that individual to be reasonably inferred by either direct or indirect means (as in data mining), including, but not limited to; name, home address, Social Security Number,

driver's license/state issued identification number, date and place of birth, mother's maiden name, biometric records, education, financial transactions, medical information, non-work telephone numbers and criminal or employment history, etc., including any other personal information that is linked or linkable to an individual. (DOT Information Technology and Information Assurance Policy Number 2006-22 (revision 1): Implementation of DOT's Protection of Sensitive Personally Identifiable Information. PII that is released for unauthorized use is likely to result in substantial harm to the individual to whom such information relates. The Department of Transportation has defined PII to mean:

Social Security Number (SSN)

- or -

The first and last name, and home address, and home telephone number of an individual, in combination with any of the following related to an individual:

- Driver's license/state-issued identification number
- Taxpayer Identification Number (TIN)
- Financial information
- Security code
- Access code
- Password
- Personal Identification Number (PIN)
- Medical information protected under the Health Insurance and Portability Accountability Act of 1996 (HIPAA) Privacy Rule
- Biometrics
- Investigations, including a report or database which contains sensitive information which can link an individual to any item above

In addition to applying the combination rules stated above, any of these items in combination with each other or alone, must be reported if mishandled or mismanaged.

(DOT Information Technology and Information Assurance Policy Number 2006-22 (revision 1): Implementation of DOT's Protection of Sensitive Personally Identifiable Information (PII))

Privacy Act Information: For purposes of the Privacy Act, information is any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

Record: Any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

System of Records: A group of any records under the control of an agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or

12/17/08

1280.1B
Appendix A

other identifying particular assigned to the individual. Please see:
www.dot.gov/privacy/privacyactnotices/

Appendix B. Personnel Records Management Guidance for Managers

Human Resource Management Offices will provide guidance to managers regarding preparation, maintenance, safeguarding, and disposition of records described below consistent with the provisions of 5 CFR 293 and this order regarding safeguarding of personnel records.

- 1. Informal Files.** Copies of written admonishments or record of verbal admonishment (warning, counseling, etc.), leave restrictions, notice of an Opportunity to Demonstrate Performance (ODP) are maintained by the manager taking the action and information copies of these documents may be maintained in the servicing Human Resource Management Office (HRMD). These records are forwarded to the servicing HRMD if they serve as material relied upon if a Disciplinary or Adverse Action File is created in this office.
- 2. Disciplinary or Adverse Action Files.** Copies of sustained reprimands, proposed disciplinary or adverse actions; material relied upon to support the action; employee replies and any documentation supplied; decision letters; the result of any third party decision pertaining to the action (e.g., administrative grievance, negotiated grievance, Merit System Protection Board (MSPB) appeal, Guaranteed Fair Treatment (GFT) appeal, Equal Employment Opportunity (EEO) complaint, Court decisions are maintained by the servicing Human Resource Office. The official record will be corrected to reflect the appropriate third party decision.
- 3. Administrative Grievances.** Records associated with an Informal grievance (paragraph B.1) pertaining to any matter of dissatisfaction to the employee, other than those for disciplinary actions, are maintained by the Deciding Official (DO). Should the employee elevate the grievance to the Formal (Step 2) level, the Informal Grievance File will be forwarded to the Grievance Deciding Official (GDO). The Formal Grievance File to include any Fact-Finding report will be maintained by the GDO.
- 4. Negotiated Grievance Files.** Grievance and arbitration files are maintained in the servicing Human Resource Office. Union filed grievances and arbitrations pertaining to unfair labor practices/complaints, a specific subject matter or contract agreement, etc., are not subject to the Privacy Act. Individual filed grievances that are maintained or can be searched by name or Social Security Number are subject to the Privacy Act.
- 5. Managerial Notes.** Managers may retain personal notes that they have authored pertaining to good or poor performance or conduct. Although these are in the possession of the manager and used in performing official functions, they are not FAA records for purposes of the Privacy Act, unless circulated. For instance, if a manager provides these notes to a Human Resources Specialist for the purpose of initiating an official FAA action, the notes become subject to the Privacy Act. Uncirculated personal notes are not subject to the control of the FAA and are retained or discarded at the discretion of the manager. For example, should a manager review their memory jogger notes to prepare a performance appraisal, the notes may then be discarded by the manager. Government equipment, such as computers or file cabinets, may not be used in the creation or maintenance of these records.
- 6. Employee Relations Tracking System (ERTS).** Records and tracking database used to track the numbers and types of actions for which there are paper files related to informal and

formal disciplinary and adverse actions taken against employees. Cases are tracked by sequentially assigned number by the HRMD entering the information, although searches can be accomplished by name.

7. Grievance Tracking System (GETS). Records and tracks both union-filed and employee-initiated negotiated grievances on any topic authorized by the governing contract. Cases are tracked by sequentially assigned numbers although searches can be accomplished by name.

8. Other Records. These include: Copies of employee's Performance Evaluation Records, Individual Development Plans; training accomplishments, including employee's performance on specific projects, details, or assignments; notes on employee performance; recognition and awards materials; attendance and leave (which are separate from the time and attendance system); notes on counseling sessions and conduct discussions; copies of debt complaint correspondence; copies of the manager's response to reference inquiries; and copies of employee's Notification of Personnel Security Action, indicating the employee's security clearance.

9. Reference Inquiries. Managers 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. Any disclosures from information contained in personnel records, maybe made only in accordance with the provisions of Chapter 4.7.

Appendix C. Privacy Records Management Processes and Procedures Guidance

This appendix is intended to be a supplemental resource to Chapter 3 in this Order. The information contained in this document originates primarily in public law.

The FAA Privacy Officer will provide additional supplementary guidance to managers regarding access and disclosure, corrections, appeals, civil remedies and criminal penalties, and guidance for fees associated with privacy records in support of this order.

1. Disclosure without Prior Written Consent. Under 5 U.S.C. 552a (b), 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 that would be required to be released under the Freedom of Information Act (FOIA) [If, under the FOIA, disclosure of the requested information is not required, the consent of the individual must be obtained prior to disclosure unless one of the following rules apply];

c. Disclosure for a routine use, provided the routine use has been established and described in the public notice required by the Privacy 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 FAA with advanced adequate written assurance that the record must 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;

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 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 obtaining consent of the individual to whom the record pertains might result in a delay that 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 on 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 Government Accountability Office;

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

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

2. Records originated outside the FAA. When a record is requested that is contained in a system of records maintained by the FAA, but which originated in another Federal agency, the Information Steward must:

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 (see originating agency's systems notice for location of organization);

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 Privacy Act of 1974, and notify the requester of the action taken (notification must include a contact person and phone number) while he/she 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 which case consultation with the originating organization is required before notification or release of the information takes place).

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 that is contained in a system of records, the FAA must:

(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 1270.1, Freedom of Information Act Program.) The following excerpt from the OMB guidelines should be applied in making this determination:

“...agencies should treat requests by individuals for information pertaining to them 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; and

(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 FAA must 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.

d. Any FAA employee receiving a request for access to a record, whether in person or by mail, must ensure prompt processing of the request, including necessary referrals if required.

e. 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. Individuals are not required to state a reason or otherwise justify the need to gain access to their own records.

4. Handling Requests for Records and Corrections.

a. Requests from Individuals for Records Pertaining to Themselves.

(1) Individuals may request access to their records in person or in writing.

(2) If the requested record is exempt from access, the Information Steward informs the individual:

(a) Of the reason why the record is exempt, citing the DOT regulation or the Privacy Act provision for the exemption; and

(b) That the exemption may be appealed to the Assistant Administrator for Information Services.

b. If the request is made in writing, the Information Steward must inform the individual of the reason for the exemption and the right to an appeal, in writing. If the request is made in person, the manager can provide that information verbally, or in writing if requested.

c. If the DOT regulation does not specifically exempt a record from access, and there is no Privacy Act provision that prohibits access, the Information Steward proceeds with the following steps to release the record to the requesting individual. (Any decision to deny access must

receive concurrence from 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 must 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. Obtains from the individual additional information to process the request

(2) 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 must 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 Office of the Secretary of Transportation General Counsel, C-1. Requests for concurrence of C-1 must be processed through the FAA Office of Aviation Medicine, AAM-1, and the Office of the Chief Counsel, AGC-1.

(3) If the request is made in person and another person accompanies the individual, he must obtain a written authorization from the individual to divulge to and/or discuss the record with or in the presence of the accompanying person.

(4) 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 C.10) and transmits the copy of the record as soon as the fee, if required, is received.

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

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

5. Third Party Requests. Information from a Privacy Act system of records from a third party (person or organization) is limited to the disclosure provisions identified in Appendix C-1. If none of the disclosure provisions apply, the request is subject to the provisions of the Freedom of Information Act.

a. If the request is not accompanied by an appropriate signed release or if not otherwise grantable under any one of the provisions of paragraph C-3, then the request is denied.

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

c. If the request is denied the Regional or Center Assistant Chief Counsel, or Chief Counsel, must be consulted to determine whether the denial should be upheld. If the denial is upheld, the procedures for appeal as described in Appendix C-7 must be included in a response letter to the requesting party.

6. Corrections to Records.

a. Requests for corrections to records must be made to the Information Steward in writing. The Information Steward must acknowledge in writing all requests to amend a record within ten working days of receipt of the request, and must either promptly inform the individual of the decision or indicate when a decision will be forthcoming.

b. The Information Steward determines if there is sufficient documentation to act on the request for amendment. If there is not, the Information Steward asks for additional documentation from the requester. The determination to amend the record is based on whether the existing record is accurate, relevant, timely, or complete. If the Information Steward determines that the record should be amended, the Information Steward performs the following:

(1) Amends the record or initiates the action to have the record amended;

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

(3) Notifies persons or agencies to which the record has been disclosed that the record has been amended and indicates the substance of the amendment; and

(4) Establishes such files as may be necessary for follow-up or reporting purposes.

c. If denial is recommended, provides appropriate legal counsel with the request for amendment, fully detailed reasons for denying the request, and a proposed letter to the requester denying the request.

d. If legal counsel concurs in the denial, the Information Steward sends the letter of denial to the individual.

7. Appeals to Privacy Act Requests.

a. **Advising Requester of Rights to Appeal.** The following procedures must be followed if an initial determination is made that access is not to be granted or a record is not to be amended:

(1) The Information Steward sends the requester a letter containing the reason for the denial and the name and position title for each person responsible for the denial, and informing the requester that appeals must be made in writing and must include all relevant documentation. Appeals should be made within 30 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.

(2) 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 must 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 employee as an appeal under the Privacy Act and has been received by the appropriate office.

(3) 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 chapter 4, paragraphs 12.b(2) or 13.h(2).

(4) When the record in question is not a personnel record, advise the requester that the letter should be addressed to the Chief Information Officer (AIO-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.

b. 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 FAA Privacy Officer must 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.

c. AIO-1 is the person who will receive the appeal.

d. AIO-1 will forward the appeal to the FAA Privacy Officer who must:

(1) Maintain a log of all appeals;

(2) Obtain the appropriate background from the office that issued the initial denial, and obtain any other information needed by the Office of the Chief Counsel to prepare a response to the appeal; and

(3) File copies of the completed determination letters.

e. The Office of the Chief Counsel, Litigation Division, AGC-400, must 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 AIO-1, unless AIO-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 must be processed through the FAA Privacy Officer.

f. Based on AGC's recommendations, the following actions must occur:

(1) If the recommendation is to grant access, initiate action to have access granted, and prepare a response for AIO-1 signature, to the requester advising him or her of the decision. The response should be processed through the FAA Privacy Officer.

(2) If the recommendation is to correct the record as requested, initiate action to correct the record, prepare a response for AIO-1 signature to the requester, attaching a copy of the corrected record or the change order initiated. The response should be processed through the FAA Privacy Officer.

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

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

(b) Establish such files as may be necessary for follow-up 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 must be performed by AGC-400:

(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 must 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;

(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

(4) Appeal to correct a record. Any statement of disagreement which the individual files must 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. Prior recipients of the disputed record must be provided a copy of any statement of disagreement to the extent that an accounting of disclosures was maintained; and

(5) 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 the Assistant Administrator for Information Services and Chief Information Officer (AIO-1) for final decision and signature.

g. AIO-1 or, if applicable, the Administrator or Deputy Administrator, will 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.

h. The Privacy Officer must notify the appropriate organizational Privacy Coordinator in the office responsible for the initial denial of the action taken on the appeal.

8. Civil Remedies.

a. Description of Circumstances. This paragraph describes the circumstances under which an individual may seek court relief in the event that the FAA violates any requirement of the Privacy Act or any rule or regulation promulgated there under. It should be noted that an individual might 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 C-9, Criminal Penalties;

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

b. Civil Action by Individuals. 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 the FAA 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 FAA action based upon an improperly constituted record; or

(4) Was otherwise injured by an FAA action in violation of the Privacy Act

c. Judicial Review of the FAA'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 Chapter 4.13 or Appendix C-3 under the following conditions:

(1) The individual has exhausted all administrative recourse under the procedures established by FAA pursuant to Chapter 4.13 or Appendix C-3, and the Agency has refused to amend the record; and

(2) 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 Privacy Act.

d. Judicial Review of the FAA's Denial of Access to a Record.

(1) 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 Chapter 4-12.

(2) The actions giving rise to the suit may be the FAA'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 Privacy Act]" (OMB Guidelines). It should be noted that particular systems of records might be exempted from the requirement of access.

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

(4) No test of injury is required to bring action under this provision.

e. Judicial Review of the FAA's Failure to Maintain a Record Properly.

(1) An individual may bring a civil action against the Government if the FAA 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.

(2) An adverse determination is one resulting in the denial of employment or a right, benefit, or entitlement by the FAA.

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

f. Judicial Review of other Failures of the FAA to Comply with the Privacy Act of 1974.

(1) In addition to the grounds specified in paragraphs C-8a-e, an individual may bring an action for any other alleged failure by the FAA to comply with the requirements of the Privacy Act or failure to comply with any rule published by the FAA to implement the Privacy Act, provided it can be shown that:

- (a) The action was "intentional or willful;"
- (b) The FAA's action had an "adverse effect" upon the individual; and
- (c) The "adverse effect" was causally related to the FAA's actions.

Note: Quotes are from OMB Guidelines.

9. Criminal Penalties.

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

b. 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 described in Appendix C-1.

c. 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.

d. 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 pretense.

10. Fees. The guidance for fees is contained in 49 C.F.R. Part 10, Maintenance of and Access to Records Pertaining to Individuals:

a. General. Subpart 10.71 prescribes fees for services performed for the public under this part by the Department.

b. 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.

| | |
|--|---------|
| (1) Copies of documents by photocopy or similar method: Each page not larger than 11 x 17 inches: | |
| First page | \$0.25 |
| Each page | \$0.05 |
| (2) Copies of documents by typewriter: Each page | \$2.00 |
| (3) Certified copies of documents: | |
| With Department of Transportation seal | \$3.00 |
| True copy, without seal | \$1.00 |
| (4) Photographs: | |
| Black and white print (from negative) | \$1.25 |
| Black and white print (from print) | \$3.15 |
| Color print (from negative) | \$3.50 |
| Color print (from print) | \$6.25 |
| (5) 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 must 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.

| | |
|--|--------|
| (6) Micro reproduction fees are as follows: | |
| Microfilm copies, each 100 foot roll or less | \$3.75 |
| Microfiche copies, each standard size sheet (4" x 6" containing up to 65 frames) | \$0.15 |
| Aperture card to hard copy, each copy | \$0.50 |
| (7) 16mm microfilm to hard copy: | |
| First | \$0.25 |
| Additional | \$0.07 |
| (8) Computer line printer output, each 1,000 lines or fraction thereof | \$1.00 |

11. 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; or

(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(b)(8) regarding computer line-printed charges.

12. Office of Personnel Management (OPM) Fees. Guidance for OPM fees is contained in 5 C.F.R. Part 294.109.

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 the requester's needs at a lower cost. Upon agreement to pay the required fees, OPM will further process the request.

(4) As described in 5 C.F.R. Part 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.

(6) 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.

(7) 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.

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

(9) 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.

(10) 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 483(a) or other applicable statutes.

(11) 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 483(a) 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 (f)(4) of this section, and the first-2-hours manual records search exception in paragraph (f)(5) of this section.

| | |
|---|---|
| Employee time | Salary rate plus 16% to cover benefits. |
| Photocopies (up to 8 1/2" x 14") | \$0.13 per 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 requester's 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.)

(4) First 100 pages of paper copies. There will be no charge to categories of requesters for the first 100 pages of paper copies, size 8 1/2" by 11" or 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.

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

(6) 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.

(7) 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 two hours of the salary of the person performing the search (i.e., the operator), OPM will begin assessing charges for computer usage.

Appendix D. Guidance for Chapter 3.2, Disclosure and Access to Records

This Appendix captures requirements from public law and other prevailing guidance that provide specific guidance and processes for disclosure and access, and is intended to provide Information Stewards with sufficient detail to assist them in carrying out their responsibilities defined in Chapter 3.2 of this order.

1. 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 that is used to collect privacy information must contain all the elements described in the following general rules.

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 intended use of the information;
- (3) The routine uses which may be made of the information; and
- (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 FAA employee in the course of his or her official duties will 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 must 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 must 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 FAA employee requesting an SSN from an individual must inform the person:

(a) That the submission of an SSN is not required by law and 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 information relating to the individual with other information about the same individual that the FAA may have in its files from previous transactions.

(d) That the SSN is solicited to assist in performing the FAA'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 3.2.(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 3.2(a), (b) and (c) 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; and

(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 Privacy Act's requirement for prior consent unless the disclosure is exempted from that requirement. (See Appendix C-1)

2. Maintenance of Records.

a. FAA will maintain all records that 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, the FAA must make reasonable efforts to ensure that such records are accurate, complete, timely, and relevant for the requesting agency's purposes.

c. The FAA must 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. Records Made Available Under Compulsory Legal Process. The FAA must make reasonable efforts to serve notice on an individual when any record on the individual is made. Subsequent justification for approval would need to contain the following: The purpose and legal authority available to any person under compulsory legal process when the 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.

4. 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 databases 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 restrictions, duplication and redisclosure restrictions, record accuracy information, and Comptroller General access statement. FAA organizations wishing to initiate computer matching programs must submit a proposal to the FAA Data Governance Board. It will decide whether to approve sending the computer matching request to the DOT Data Integrity Board for approval. (The DOT Data Integrity Board is made up of the DOT Chief Information Officer, DOT General Counsel, and DOT Inspector General). The approval process includes information to assess records accuracy in order to provide a reasonable assurance of fairness in use of the data and to enable cost-beneficial use of the exchanged data. The review process may also include a requirement that a benefit/cost analysis be completed. Once approved, a computer matching program is reviewed annually. There is also a requirement to publish matching notices in the Federal Register.

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 FDGB through AIO-1, as a co-chair (and AIO's Information Management Division as executive secretary), and request a review of the proposed matching program.

d. OMB published "Final Guidance Interpreting the Provisions of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1988, 54 FR 25818" on June 16, 1989. This is available from the OMB web site (currently <http://www.whitehouse.gov/omb/privacy/matching.html>). It describes the information required in a computer matching program proposal (for submission to the FDGB and DOT Data Integrity Board)

5. Transfer of Records other than to Federal Records Centers. Procedures established in the current version of Order 1350.14, Records Management must be followed. This transfer of records constitutes a disclosure and an accounting is required.

6. Records Safeguards. Chapter 3.4, Safeguarding Policy, 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 that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

7. Transfer of Records.

a. **Federal Records Center.** Each record transferred must, for purposes of the Privacy Act, be considered the property of FAA. The National Archives and Records Center (NARA) must 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, must 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, will be considered the property of the National Archives and not be subject to many of the provisions of the Privacy Act; however, such records must be included in the systems of records notice published in the Federal Register. Each office must examine its records of transfer to ensure compliance with this provision of the Privacy Act. Offices must 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.

8. Accounting of Certain Disclosures. The Privacy Act of 1974 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 FAA 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. 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 nature was actually disclosed; and

(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.

b. Disclosure Accounting Requirements. Managers of systems of records must:

(1) Keep an accurate accounting of:

(a) The date, nature, and purpose of each disclosure of a record to any person outside DOT or to another agency; and

(b) The name and address of the person or agency to which the disclosure was made.

(2) 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.

(3) 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 Privacy 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 Privacy Act.

(4) 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.

(5) No standardized form or format will be prescribed for this purpose. However, an existing form, FAA Form 1300-11, History, NSN (National Stock Number) 0052-00-8 08-9000, Unit of Issue: Sheet, could be used depending upon the nature of the system. Other Information Stewards may find plain, white paper satisfactory for logging information that meets the disclosure accounting requirement. For automated systems, an automated accounting system must be developed.

c. Procedures for Disclosure Accounting.

(1) Requests from an individual for an accounting of disclosures from his/her records must 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 must maintain a record of all disclosures and related activities.

Appendix E. Reporting Incidents

1. Purpose. This appendix gives guidance for reporting thefts, losses, or unauthorized disclosures of Personally Identifiable Information (PII). This guidance enables the FAA to determine the impact; if any of a theft, loss, or unauthorized disclosure to the subject individual and to the agency.

2. Determine the nature of the event.

a. Source: Is the PII collected or maintained by or on behalf of the FAA? If the FAA is the source of the PII, the event merits reporting in accordance with this policy.

b. Circumstances

(1) Was the PII disclosed without consent of the subject individual? An event in which an individual consents to, or willingly discloses their own PII, does not merit reporting in accordance with this policy.

(2) Was the PII disclosed to person(s) other than DOT employee(s) who need to use the records when performing their duties? The provisions of this policy do not preclude disclosure of PII without consent to DOT employee(s) who need to use the records when performing their duties. It is a privacy incident if an employee's data is disclosed to another DOT/FAA employee without a need to know.

c. Sensitivity:

(1) Does the PII identify a person by a Social Security Number (SSN)?

(2) Does the PII identify a person by first and last name, home address, home telephone number, in combination with any of the following related to an individual:

- (a) Driver's license/state-issued identification number
- (b) Taxpayer Identification Number (TIN)
- (c) Financial information
- (d) Security code
- (e) Access code
- (f) Password
- (g) Personal Identification Number (PIN)
- (h) Medical information

(i) Biometrics

(j) Investigations, including a report or database which contains sensitive information which can link an individual to any item above.

Note: All PII exposures must be reported to the DOT Cyber Security Management Center (CSMC) immediately upon discovery.

3. Report the incident. Provide the following information regarding PII exposures to the CSMC immediately upon discovery. The lack of complete information must not prevent the reporting of PII exposures.

- a. Name and contact information of the person reporting the PII exposure.
- b. Line of business owner of the equipment, media or data file.
- c. Owner or custodian of the equipment, media or data file.
- d. Time (specify time zone) and date of the PII exposure.
- e. Location of incident occurrence
- f. Type of PII attributes/data elements that were exposed
- g. Incident details: (i.e., unauthorized access, theft, data compromise)
- h. Individuals involved (i.e., sender, recipient, data owner)
- i. Impacted Systems (i.e., laptop, USB (Universal Serial Bus) drive, disk drive, documents, etc.)
- j. Protection mechanisms (i.e., password, encryption, no protection)
- k. Any initial mitigation steps taken to contain the incident (i.e. system taken offline, cached data deleted)
- l. Reports made to law enforcement/Inspector General (jurisdiction, contact information and report identification number)

4. After completing the initial report. In addition to the information in paragraph 3 above, determine the following:

- a. Where did the information exist: laptop, desktop system, server, personal digital assistant (PDA), wireless handheld devices, removable disk drives, CD-ROMs, DVDs, USB memory sticks, floppy disks, magnetic tape, paper documents, and any other form.

b. Describe the nature of the incident (for e.g., laptop stolen from rental car, Blackberry left on train, fax copy compromised, or briefcase lost with airman certification and health records).

c. What was lost, or stolen, or compromised (e.g., laptop, USB memory stick, or paper documents, computer file)?

d. Date or time that someone first noticed the equipment or media missing, or electronic files compromised. Specify GMT, local, or time zone.

e. Where did the incident take place (FAA facility, office, home, car)? In the case of electronic data compromise, how was the accidental transmission or intrusion detected?

f. Where was the equipment, or media, or data file when the incident occurred (e.g., car trunk, hotel room, locker room etc.)?

5. About the Equipment, or Media, or electronic data:

a. What line of business or staff office owned the equipment, or media, or data file?

b. What FAA program or system did the equipment, or media, or data file support?

c. Provide a list of all users of the equipment, media, or data device.

6. About the PII:

a. What software was installed on the equipment?

b. What data was on the equipment or media, such as Word documents, investigative reports, databases, etc?

c. What PII was on the equipment or media, such as address, Social Security Number, driver's license or state-issued identification number, taxpayer identification number, financial information, security code, password, personal identification number, medical information, biometrics, investigative reports, etc.

d. How was the data obtained (e.g., downloaded from an FAA site, inputted by the equipment user, notes from interviews, etc.)

e. Was a backup of the information made before the equipment was lost or stolen?

f. What protections were in place on the backups to ensure that the integrity of the backups has not also been compromised?

7. About Equipment Network Access:

a. Was the equipment used to access an FAA or other government system, and if so what systems did the user or user access with the equipment?

b. Where are these systems located?

c. Did any application of the equipment automatically log a user on to an FAA or other government system?

d. Were any user IDs and password stored on the equipment or media.

e. Do the equipment's users access any FAA or other systems containing PII data?

8. About Data Safeguards:

a. Was a logon ID and password needed to access the equipment?

b. Do data backups exist?

c. Were they password protected?

d. Who has access to the logs?

Appendix F. Security Controls For Protection Of PII

The security controls in this chart apply to manual and electronic systems of privacy records. Security controls include administrative processes, procedures, devices, techniques and technologies that reduce the risks to information and information systems in relation to the vulnerabilities and validated threats, to an acceptable level. System owners must use this checklist to evaluate the privacy controls implemented in their information systems. If you have questions about manual security controls contact your `Servicing Security Element (SSE). In regions your SSE is the Security and Hazardous Materials Division, Axx-700, and at the Washington Headquarters, your SSE is the Office of Security, AIN-1. If you have questions about electronic security controls contact the Office of Information Systems Security, AIS-1.

| Controls | • Mandatory | ▲ Optional |
|--|--------------------|-------------------|
| Management Controls | | |
| Reduce volume of PII in your records. | • | |
| Eliminate social security numbers as a personal identifier to identify a person in a record, unless approved by FAA CIO. | • | |
| Assign an impact level to a record system: moderate or high impact to PII records per FAA Order 1280.1, Chapter 3.4.e. | • | |
| See intranet privacy site for an information system security plan template for paper records. For electronic records see Certification and Accreditation Handbook. | • | |
| Personnel Security Controls | | |
| Before giving access to an employee or contractor, ensure the employee or contractor satisfies background investigative requirements. | • | |
| Marking Controls | | |
| Mark documents to draw a reader's attention to the record's sensitivity. | • | |

| Controls | • Mandatory | ▲ Optional |
|--|--------------------|-------------------|
| Storage Controls | | |
| When not under physical control of an authorized person, store PII records in a locked container, such as, a lockable filing cabinet, Lektriever, GSA approved security container, or in a secure room equipped with an FAA approved locking system. | • | |
| Control keys to locked containers and secure rooms and key holder must be people who are authorized access to records. | • | |
| Protect secure rooms with an electronic intrusion detection system. | | ▲ |
| Protect systems connected to a network with electronic intrusion detection. | • | |
| All PII data stored or carried on a FAA-owned mobile computer or FAA-owned storage devices/media must be encrypted using the FAA CIO-approved and recommend encryption. | • | |
| Access Controls | | |
| Ensure recipients of records have an approved need to access your privacy information. Ensure the appropriate controls are in place to protect PII provided and that there is a need to know your privacy information. | • | |
| When privacy records are not in secure storage, they must be under the physical protection and control of an authorized person. This person must take reasonable steps to prevent inadvertent disclosure of the record to unauthorized persons per FAA and Federal requirements. | • | |
| When privacy records are in hard copy, protect them with a cover sheet such as FAA Form 1600.80 and store them in a locked file cabinet, or in other FAA approved secure storage items, to prevent inadvertent or casual disclosure. | | ▲ |
| Restrict access so that unauthorized personnel will not be able to view sensitive information displayed on monitors. Privacy information should not be displayed on public monitors and the appropriate controls should be in place to hide the privacy information via the use of special characters. | | ▲ |
| Telephone, Fax, and Email Controls | | |
| When using voice communications, verify the person requesting such information is authorized by requesting their name, title, reporting organization, manager's name, contact information, requesting the purpose for collecting such information, and discussing the intent of the information before discussing PII. | • | |
| When using fax communications, mark your fax to draw attention to its sensitivity; use special care to ensure you are sending documents to the correct fax number; and find out how your fax is handled at the receiving end. | • | |

| Controls | ● Mandatory | ▲ Optional |
|--|----------------|------------|
| If you are sending the fax to a controlled area, where only authorized persons will have access to it, then you may send it without further precautions, or If you are sending the fax to an uncontrolled area, where unauthorized persons might have access to the fax, then request that an authorized person stand by at the receiving end as you send the fax, and ask them to confirm its receipt. | | |
| If sending an imaged document by email within the FAA email domain, use the email system's (currently Lotus Notes) encryption option to protect the document. Notify the receiver of the documents sensitivity. Digitally sign the email so the receiver can validate the authenticity of the email and of the sender. | ● | |
| If sending an imaged document by email outside the FAA email domain, encrypt the image with FIPS approved encryption. | ● | |
| Reproduction Controls | | |
| Restrict reproduction to the extent needed to carry out official duties. | ● | |
| Mark, handle, and protect copies in the same manner as the originals. | ● | |
| Removable media will be clearly marked and encrypted at origination containing PII | ● | |
| Off-site storage used to house backup media need to meet physical and environmental protection requirements specified by the media manufacturers for long-term storage. | ● | |
| Sanitize removable/reusable media before re-use based on the criticality of the information per FAA Order 1370.100 (Media Sanitizing and Destruction Policy). Criticality is classified as low, moderate, or high impact as defined in FIPS 199. | ● | |
| Distribution of PII by Hand carriage, Mail Channels and Commercial Carriers | | |
| If hand carrying PII outside your administrative space, put the information in an opaque envelope or carry it within a locked brief case or other container and keep it under your possession and under your control. Ensure a coversheet is placed in front of the information. | ● | |
| When sending PII by interoffice mail, protect it with a sealed opaque envelope, such as, FAA Form 1360-39, For Official Use Only envelope. Be sure to clearly address the envelope(s), and reinforce the seams and closures on the envelopes/containers to prevent loss or spillage of PII data in the event the package is handled roughly and exposed to damage. Verify the envelope is addressed correctly, and confirm delivery. | ● | |
| When shipping or mailing PII to another facility, protect the | ● | |

| Controls | • Mandatory | ▲ Optional |
|---|----------------|------------|
| information in properly addressed opaque envelopes or containers and include a cover sheet. Be sure to clearly address the containers, and reinforce the seams and closures on the envelopes/containers to prevent loss or spillage of PII data in the even the package is handled roughly and exposed to damage. Ship or mail by United States Postal Service Registered, Express, Certified or first class, or by an approved GSA contracted commercial delivery service. | | |
| When transporting, mailing or shipping PII on electronic media to another facility, the data/media must be encrypted using authorized DOT/FAA software and procedures. The key to decrypt the data will not be sent in the same container/transmission as the encrypted data. | • | |
| Telecommuting Controls | | |
| Personnel working with agency records containing PII in telecommuting environments must meet all required security controls and procedures for protection of such data. Custodians must approve specific security controls for storing and handling paper records at home and while traveling. | • | |
| Acquisition Controls | | |
| If you use contract support to administer you system of records, ensure your support contract have appropriate security clauses from the FAA Acquisition System Toolset (FAST).Additional information can be found in section 3.7 of: http://fasteditapp.faa.gov/ams/do_action | • | |
| Disposition and Destruction Controls | | |
| Retain and retire records by the guidelines and procedures of FAA Order 1350.15 (Records Organization, Transfer, and Destruction Standards). | • | |
| Ask your supporting SSE, for assistance in selecting an appropriate destruction method and equipment before destroying paper documents. | • | |
| "Any identifying labels on storage media that indicate the nature and sensitivity of their contents must be removed or rendered unreadable when the media are sanitized." (DOT IT/IA Directive 034) Destroy, clear, or sanitize electronic media by NIST standards and guidelines, and other applicable Federal requirements. | • | |
| The written record must include: The name(s) of the individual(s) who performed the disposal action, what action was taken (e.g., how the media was sanitized and destroyed), and when the action was taken. See FAA Order 1370.100 (Media Sanitizing and Destruction Policy). | • | |
| All storage media and devices that contain, or may have | • | |

| Controls | • Mandatory | ▲ Optional |
|---|--------------------|-------------------|
| contained, privacy information must be sanitized when no longer needed. Sanitization must be conducted in accordance with applicable Federal laws and regulations, Department of Commerce standards and guidelines, and Departmental and FAA policy. | | |
| Incident Planning and Reporting Controls | | |
| When PII is disclosed to unauthorized person, report the incident to the FAA's Cyber Security Management Center (CSMC) within one hour of discovering an incident. 2. OMB 07-16 requires DOT/FAA to notify DHS on all PII disclosure within one hour of the incident. | • | |
| Plan for protecting or reconstituting PII records during cyber forensics, emergencies, and Continuity of Operations Plans (COOP) | • | |

Appendix G. Information System Security Plan for Records Systems

1. Guidance for the Information System Security Plan. This appendix gives you guidance for preparing an information system security plan for a manual or paper system of privacy records. If your system of records is electronic see FAA Order 1370.82, Information System Security Program, or your Information Systems Security Manager (ISSM) for guidance on preparing an ISSP.

2. Purpose. By FAA Order 1280.1, each information steward for a Privacy Act system of record must have a plan for protecting those records. This plan sets up security controls (per NIST SP 800-53) and procedures for protecting the privacy records managed by the Information System Owner or Information Steward. Information Stewards must use FAA form 1280.1.

3. Description of the System of Records.

- a. Provide a name, description, and storage media of the system.
- b. Identify the record system in which you keep personally identifiable information (PII). Describe how PII is received, handled, stored, accessed, sent, destroyed, and records retired.
- c. List the internal and external organizations that access the records.
- d. List any laws, regulations, or reason for setting up the records.
- e. Include a statement of the estimated risk and magnitude of harm from loss, misuse, or unauthorized access of records.

4. Persons Responsible for This System of Records.

- a. List the individual or individuals, by position, who have managerial responsibility for the records.
- b. List the individual or individuals, by position and organization who are responsible for the security of the system.
- c. List the employees by position and contractors by role who by position protect the system.

5. Marking Controls. If you mark documents in your system of records, discuss what documents you mark and how you mark them.

Note: Marking is a basic protective measure to draw a reader's attention to the sensitivity of information and the need to protect it.

6. Access Controls.

- a. Describe the people who may have access and describe limits on their access if any.

b. Describe how you limit access to authorized people during working hours and after working hours.

c. Describe the authentication technologies used on the system to protect data while stored or in transit.

d. Describe authentication methodology used on the system to ensure that only authorized users are able to access PII data.

7. Acquisition Controls.

a. If you have supporting contracts for your system of records, list those contracts.

b. Ensure your contracts have proper security clauses from the FAA Acquisition System Toolset (FAST).

c. Ensure the contractors and their employees have completed an appropriate nondisclosure agreement (NDA).

d. Ensure contractor employees have a proper position sensitivity designation and have undergone a background screening appropriate for their positions. See FAA Order 1600.72, Contractor, and Industrial Security Program.

8. Storage Controls.

a. When privacy records are not under the physical custody or control of an authorized person, you must store it in a lockable container, such a security container, Lektiever, filing cabinet, desk or locked space. Describe how you store records that are not under the physical custody or control of an authorized person.

b. Describe how you control keys to containers and spaces. Key holders must be people who have authorized access to your records.

9. Transmission and Shipping Controls.

a. When mailing or shipping records, describe how you protect documents and records during shipping.

b. When sending records through interoffice mail, describe how you protect documents and records.

c. When faxing documents describe your procedures for protecting faxes during transmission.

10. Disposal and Destruction Controls.

- a.** You must retain and retire records by the guidelines and procedures of FAA Order 1350.15 (Records Organization, Transfer, and Destruction Standards).
- b.** You must transfer and destroy your records in accordance with FAA Order 1370.100 (Media Sanitizing and Destruction Policy).
- c.** You must completely destroy paper records containing PII. Destruction can be accomplished by shredding, burning, pulping, pulverizing, or some other method that assures destruction beyond recognition and reconstruction.
- d.** If you store any of your paper records on electronic media like hard drives and compact disks, you must sanitize them in accordance with applicable Federal laws and regulations, Department of Commerce standards and guidelines, and Department of Transportation and FAA policy.
- e.** You must retain records of the methods and procedures you used for sanitizing and destroying media that contained or may have contained PII either hard or soft copy in accordance with FAA Order 1350.15, Records Organization, Transfer, and Destruction Standards.

11. Privacy and Security Awareness and Training.

- a.** Describe the awareness training (formal classroom, on-the-job training, and employee meetings).
- b.** Annual training is required of all personnel. Awareness training must describe the criminal or administrative penalties for unauthorized disclosures

Appendix H. Privacy Impact Assessment (PIA) Template

**DEPARTMENT OF TRANSPORTATION
Federal Aviation Administration
Office of (Insert)**

PRIVACY IMPACT ASSESSMENT

**System Name
(Web site, if applicable)**

Date

System Overview

The Federal Aviation Administration (FAA), within the Department of Transportation (DOT), has been given the responsibility to carry out safety programs to ensure the safest, most efficient aerospace system in the world. The FAA is responsible for:

- Regulating civil aviation to promote safety;
- Encouraging and developing civil aeronautics, including new aviation technology;
- Developing and operating a system of air traffic control and navigation for both civil and military aircraft;
- Developing and carrying out programs to control aircraft noise and other environmental effects of civil aviation; and
- Regulating U.S. commercial space transportation.

One of the programs that helps the FAA fulfill this mission is the <INSERT SYSTEM NAME>, which <insert system purpose>.

The <INSERT SYSTEM NAME> system provides <insert basic system description>.

[system name; Component name; description of the system, its functions, and how it relates to mission]

Information, Including Personally Identifiable Information (PII), in the System

The <INSERT SYSTEM NAME> system contains both personally identifiable information (PII) and non-personally identifiable information pertaining to <insert which group(s) of people>. PII collected in the <INSERT SYSTEM NAME> system includes:

- <list PII items in bulleted format>

An individual's PII is entered into the <INSERT SYSTEM NAME> system <insert how, e.g. manually by whom or electronic transfer of information from which other system(s)>.

[data elements and sources]

Why SYSTEM NAME Collects Information

<INSERT SYSTEM NAME> collects information in order to <insert purpose>.

[program purpose(s); other considerations]

Legal Authority for Information Collection

[statute(s), Executive Order(s), regulation(s)]

How SYSTEM NAME Uses Information

Information in <INSERT SYSTEM NAME> is used <insert by whom and for what>.

[internal uses; compatibility with collection purpose; SORN(s)]

How SYSTEM NAME Shares Information

PII contained in <INSERT SYSTEM NAME> is shared with <insert individuals, organizations, and entities that receive information from this system, why they need this information, and how they receive it, e.g., hardcopy or electronic transfer of data from one system to another.>

[internal and external sharing; compatibility with collection purpose; sharing agreements; SORN(s)]

How SYSTEM NAME Provides Notice and Consent

For an individual's PII to be included in the <INSERT SYSTEM NAME>, that individual must have <insert why an individual's information would be included in the system>. <Insert information on how the system provides notice and choice, if applicable>.

[extent to which individuals are notified of the scope of information collected, can consent to uses, and can decline to provide information]

How SYSTEM NAME Ensures Data Accuracy

<Insert details of how the information is obtained (in what form and from whom) and entered into the system (how and by whom), and what steps are taken to ensure the accuracy of the data>.

Under the provisions of the Privacy Act, individuals may request searches of the <INSERT SYSTEM NAME> file to determine if any records have been added that may pertain to them. This is accomplished by <insert instructions on how individuals should make this request and the information needed, example: sending a written request directly to the SYSTEM NAME program office that contains name, authentication information, and information regarding the

request>. FAA does not allow access through either the Internet or Intranet to the information stored in the <INSERT SYSTEM NAME>.

[collection procedure; verification procedure]

How SYSTEM NAME Provides Redress

Insert information on how consumers can express grievances about privacy issues, how those issues are resolved, and how consumers have access and can change personal information. Should include some type of contact information such as the name of the person or office to contact, a mailing address or e-mail address, and a telephone number.>

[procedure allowing individuals to access and amend their information]

How SYSTEM NAME Secures Information

<INSERT SYSTEM NAME> takes appropriate security measures to safeguard PII and other sensitive data. <Insert details of system security measures>

In addition, access to <INSERT SYSTEM NAME> PII is limited according to job function. <INSERT SYSTEM NAME> access control privileges are set according to the following roles:

- <insert roles>
- <insert roles>

The matrix below describes the levels of access and safeguards around each of these roles as they pertain to PII.

<Modify the table below with the access level information pertinent to the system>

| ROLE | ACCESS | SAFEGUARDS |
|----------------|--|---|
| User (Level 3) | <ul style="list-style-type: none"> • Submit new debarment, suspension, and conviction records for designated transportation oversight entity • Change existing debarment, suspension, and conviction records for designated transportation oversight entity • Access and change own profile information | <ul style="list-style-type: none"> • User-set user name and password • Account set-up approved by User (Level 2) and Administrator (Level 1) • Passwords expire after a set period • Minimum length of passwords is 8 characters • Passwords must be combination of alpha/numeric/special characters |

| | | |
|---------------------------|---|---|
| | | <ul style="list-style-type: none"> Accounts are locked after a set number of incorrect log-in attempts |
| User (Level 2) | <ul style="list-style-type: none"> Submit new debarment, suspension, and conviction records for designated transportation oversight entity Change existing debarment, suspension, and conviction records for designated transportation oversight entity Request User (Level 3) account for designated transportation oversight entity Access and change own profile information Access and change User (Level 3) profile information | <ul style="list-style-type: none"> User-set user name and password Account set-up approved by Site Administrator (Level 1) Passwords expire after a set period Minimum length of passwords is 8 characters Passwords must be combination of alpha/numeric/special characters Accounts are locked after a set number of incorrect attempts |
| Site Administrator | <ul style="list-style-type: none"> Search and view user names and profile information Grant User (levels 2 and 3) accounts, reset account passwords, view access log information Delete profiles (without viewing full profile information) View, search, add, change, and delete all information in database | <ul style="list-style-type: none"> User-set user name and password Account set-up approved by OIG management Passwords expire after a set period Minimum length of passwords is 8 characters Passwords must be combination of alpha/numeric/special characters Accounts are locked after a set number of incorrect attempts Must access system from limited number of computers, each of which also has user name/password access control. |

[access controls; Certification & Accreditation; detection of misuse]

How Long SYSTEM NAME Retains Information

Data in <INSERT SYSTEM NAME> is maintained for <insert how long>, according to <cite applicable rule, if any>.

(Please refer to your Program Offices National Achieves Records Administration (NARA) approved schedule.)

System of Records

<INSERT SYSTEM NAME> <is/is not> a system of records subject to the Privacy Act because it is searched by <insert PII searched by, e.g., name and phone number>. You can find <INSERT SYSTEM NAME>'s system of records notice at <http://cio.ost.dot.gov/policy/records.html>, DOT/FAA, <insert SORN information>, <INSERT SYSTEM NAME>.

[whether the system is searched by personal identifier, i.e., is a Privacy Act system; SORN(s)]

Appendix I. Privacy Threshold Analysis (PTA) Template

**Federal Aviation
Administration**

The Privacy Office
Federal Aviation Administration
Washington, DC 20591
202 267-9895
www.faa.gov/privacy
Page 1 of 6

Privacy Threshold Analysis (PTA)

*Please use this form to determine whether a Privacy Impact Assessment (PIA) is required for your project/
electronic information collection system.*

Under the E-Government Act of 2002 (*P.L. 107-347*), certain FAA project/ system owners and developers are required to complete Privacy Impact Assessments ("PIAs") to determine the privacy implications of FAA projects/ systems that handle information in an identifiable form. This form is a threshold document used to help determine whether a PIA is required for your project/ system. After completing this form, please return it to the following address:

Carla Mauney
FAA Privacy Office
IT Enterprise Business Services, AES-200
Federal Aviation Administration
20591 (Room 712)
Tel: 202-267-9895
Fax: 202-267-5945
Carla.Mauney@faa.gov

Upon receipt, the FAA Privacy Office will review your response. If it is determined that a PIA is required, the FAA Privacy Office will send you a copy of the DOT Privacy Impact Assessment Template to complete and return.



Federal Aviation Administration

The Privacy Office
Federal Aviation Administration
Washington, DC 20591
202 267-9895
www.faa.gov/privacy
Page 2 of 6

Privacy Threshold Analysis (PTA)

Please complete this form and send it to the FAA Privacy Office.
Upon receipt, the FAA Privacy Office will review your response and may request additional information.

Note: For purposes of this form, all technologies/systems should be initially reviewed for potential privacy impact. There is no distinction made between national security systems or technologies/systems managed by contractors..

SUMMARY INFORMATION

DATE submitted for review:

NAME of Project/System: <Please enter the project/system name.>

Name of Project/System Manager: <Please enter the name.>

Email for Project/System Manager: < Please enter the email address.>

Phone number for Project/System Manager: < Please enter the phone number.>

TYPE of Project:

- ☐ Information Technology and/or System *
- ☐ A Notice of Proposed Rule Making or a Final Rule
- ☐ Other: <Please describe the type of project including paper based Privacy Act System of Records.>

* The E-Government Act of 2002 defines these terms by reference to the definition sections of Titles 40 and 44 of the United States Code. The following is a summary of those definitions:

- "Information Technology" means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. See 40 U.S.C. § 11101(6).
- "Information System" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44 U.S.C. § 3502(8).



Federal Aviation Administration

The Privacy Office
Federal Aviation Administration
Washington, DC 20591
202 267-9895
www.faa.gov/privacy
Page 3 of 6

SPECIFIC QUESTIONS

1. Describe the project and its purpose:

<Please provide a general description of the project and its purpose in a way a non-technical person could understand.>

2. Electronic Nature of the System:

- ☐ This Project/ System collects, maintains or disseminates information in an identifiable form¹ from/ about members of the public.
- ☐ This Project/ System initiates a new electronic collection of information in an identifiable form from 10 or more members of the public.

3. Status of Project:

- ☐ This is a new development effort
- ☐ This is an existing project
 - Date first developed:
 - Date last updated:
 - <Please provide a general description of the update.>

¹ In the E-Government Act of 2002, "information in an identifiable form" is defined as "information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.), or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements; i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator and other descriptors.)"



Federal Aviation Administration

The Privacy Office
Federal Aviation Administration
Washington, DC 20591
202 267-9895
www.faa.gov/privacy
Page 4 of 6

4. If this project is a technology/system, does it relate solely to infrastructure? [For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)]

☐ No. Please continue to the next question.

☐ Yes. Is there a log kept of communication traffic?

☐ No. Please continue to the next question.

☐ Yes. What type of data is recorded in the log?

<Please list the data elements, including information in an identifiable form, included in the log.>

5. Could the project relate to or provide information in an identifiable form about an individual and/or member of the public?

☐ No. Please skip ahead to question 6.

☐ Yes. Please provide a general description, below.

<Please provide a general description of the way the project could relate to or provide information about an individual and/or members of the public.>

6. What information about individuals could be collected, generated or retained?

<Please provide a specific description of information that might be collected, generated or retained. >

<Provide such information as: name, address, driver's license information, vehicle identifiers, biometric information, phone numbers, email addresses, cell phone numbers, medical information, financial information, employee status, certificates (e.g., birth, marriage), military status, professional licenses, etc.)>



Federal Aviation Administration

The Privacy Office
Federal Aviation Administration
Washington, DC 20591
202 267-9895
www.faa.gov/privacy
Page 5 of 6

7. Will the Project/System contain information on retired or former FAA employees?

- ☐ No.
☐ Yes. <Please provide a specific description of information that might be collected, generated, or retained such as names, addresses, emails, etc.>

8. Will the Project/System contain information on members of the public?

- ☐ No.
☐ Yes. <Please provide a specific description of information that might be collected, generated, or retained such as names, addresses, emails, etc.>

9. Was this Project/System in place prior to 2002?

- ☐ No.
☐ Yes. <Please indicate year it began>

10. Has the Project/ System been modified in any way since 2002?

- ☐ No.
☐ Yes. <Please provide a specific description of how the system has been modified >

11. Does a Certification & Accreditation exists or in development?

- ☐ Unknown.
☐ No.
☐ Yes. Please indicate the determinations for each of the following:

Confidentiality: ☐ Low ☐ Moderate ☐ High ☐ Undefined

Integrity: ☐ Low ☐ Moderate ☐ High ☐ Undefined

Availability ☐ Low ☐ Moderate ☐ High ☐ Undefined

*Projects can relate to individuals in a number of ways. For example, a project may include a camera for the purpose of watching a physical location. Individuals may walk past the camera and images of those individuals may be recorded. Projects could also relate to individuals in more subtle ways.



Federal Aviation Administration

The Privacy Office
Federal Aviation Administration
Washington, DC 20591
202 267-9895
www.faa.gov/privacy
Page 6 of 6

Privacy Threshold Review

(To be completed by the FAA Privacy Office)

DATE reviewed by the FAA Privacy Office:

NAME of the FAA Privacy Office Reviewer:

Carla Mauney
FAA Privacy Office
IT Enterprise Business Services, AES-200
Federal Aviation Administration
20591
Tel: 202-267-9895
Fax: 202-267-5945

DETERMINATION:

☐ **This is NOT a Privacy Sensitive System** – the system contains no Personally Identifiable Information.

☐ **This IS a Privacy Sensitive System**

- ☐ A SORN is required
- ☐ PTA sufficient at this time
- ☐ A PIA is required
- ☐ National Security System
- ☐ Legacy System
- ☐ HR System

FAA PRIVACY OFFICER COMMENTS

Appendix J. References

References on which this order was based, and which must be followed are listed, but not limited to, those identified in the table below.

| | REFERENCE NUMBER | REFERENCE TITLE | DATE |
|-------------------------|----------------------------------|--|-------------|
| PUBLIC LAWS | | | |
| | Public Law 93-579 | Privacy Act of 1974 5 U.S.C. § 552a | 12/31/1974 |
| | Public Law 107-296 | Homeland Security Act 2002 | 11/25/2002 |
| | Public Law 107-347 | E-Government Act of 2002 | 1/7/2003 |
| | Title III of Public Law 107-347 | The Federal Information Security Management Act of 2002 (FISMA) | 10/30/2000 |
| | Title XVII of Public Law 105-277 | Government Paperwork Elimination Act of 1998 | 10/23/1998 |
| | 5 CFR Part 297 | Privacy Procedures for Personnel Records | 01/01/2002 |
| | 44 U.S.C. 3501 updated | Government Paperwork Reduction Act of 1980 | 01/23/2007 |
| | 5 USC 552 | Freedom of Information Act Program | 12/23/2002 |
| EXECUTIVE ORDERS | | | |
| | HSPD-7 | Critical Infrastructure Identification, Prioritization, and Protection | 12/17/2003 |
| | HSPD-12 | Policy for a Common Identification Standard for Federal Employees and Contractors | 8/27/2004 |
| OMB MEMORANDA | | | |
| | OMB A-130A | Management of Federal Information Resources | 2/8/1996 |
| | OMB M-05-24 | Implementation of Homeland Security Presidential Directive (HSPD) 12 | 8/5/2005 |
| | OMB M-06-15 | Safeguarding PPI | 5/22/2006 |
| | OMB M-06-16 | Protection of Sensitive Agency Information | 6/23/2006 |
| | OMB M-06-19 | Reporting Incidents Regarding PII and Incorporating the Cost for Security in Agency IT Investments | 7/12/2006 |
| | OMB M-07-16 | Safeguarding Against and the Breach of PII Responding to | 5/22/2007 |

| | REFERENCE NUMBER | REFERENCE TITLE | DATE |
|--|-----------------------------|---|-------------|
| | OMB M-07-19 | FY 2007 Reporting Instructions for FISMA and Agency Privacy Management | 7/25/2007 |

| | REFERENCE NUMBER | REFERENCE TITLE | DATE |
|--|-----------------------|--|---------------------------|
| NIST FEDERAL INFORMATION PROCESSING STANDARDS | | | |
| | NIST FIPS 140-2 | Security Requirements for Cryptographic Modules | 5/25/2001 |
| | NIST FIPS 199 | Standards for Security Categorization of Federal Information and Information Systems | Feb 2004 |
| | NIST FIPS 200 | Minimum Security Requirements for Federal Information and Information System | Mar 2006 |
| | NIST FIPS 201-1 | Personal Identity Verification (PIV) of Federal Employees and Contractors | Mar 2006 |
| NIST SPECIAL PUBLICATIONS | | | |
| | NIST SP 800-53 Rev. 2 | Recommended Security Controls for Federal Information Systems | Dec 2007 |
| | NIST SP 800-53A | Guide for Assessing the Security Controls in Federal Information Systems | Jun 2007 (third draft) |
| 18 | NIST SP 800-61 Rev 1 | Computer Security Incident Handling Guide | 9/27/2007 |
| 19 | NIST SP 800-88 | Guidelines for Media Sanitization | Sep 2006 |
| 20 | NIST SP 800-60 Rev 1 | Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories | June 2004 |
| 21 | NIST SP 800-60 Rev 1 | Volume II: Appendixes to Guide for Mapping Types of Information and Information Systems to Security Categories | June 2004 |
| DOT ORDERS | | | |
| | DOT 2006-22 | Implementation and Protection of DOT PII | 10/11/2006 |
| | DOT H 1350.2 | Departmental Information Resources Management Manual (DIRMM) | Jan 2006 |
| FAA ORDERS | | | |
| | FAA Order 1350.14 | Records Management | 2/28/1980 |
| | FAA Order 1100.154 | Delegations of Authority | 6/12/1990 |
| | 5 USC 552 | Freedom of Information Act Program | 12/23/2002 |
| | FAA Order 1370.100 | Media Sanitizing and Destruction Policy | 10/1/2007 |
| | FAA Order 1370.82 | Information System Security Program | 9/11/2006 |

| | REFERENCE NUMBER | REFERENCE TITLE | DATE |
|----------------------|---------------------|---|------------|
| FAA ORDERS (cont'd.) | | | |
| | FAA Order 1370.93 | FAA Web Management | 8/17/2004 |
| | FAA Order 1375.1 | Data Management: Departmental Data Integrity Board | 7/25/2006 |
| | FAA Order 1600.1 | Personal Security Program | 7/25/2005 |
| | FAA Order 1600.2 | Safeguarding Classified National Security Information | 10/23/1983 |
| | FAA Order 1600.69 | FAA Facility Security Management Program | 10/1/2003 |
| | FAA Order 1600.75 | Protecting Sensitive Unclassified Information | 2/1/2005 |

Appendix K. Form 1320-19, Directive Feedback Information

Directive Feedback Information

Please submit any written comments or recommendation for improving this directive, or suggest new items or subjects to be added to it. Also, if you find an error, please tell us about it.

Subject: Order

To: Directive Management Officer, _____

(Please check all appropriate line items)

- ☐ An error (procedural or typographical) has been noted in paragraph _____ on page _____.
- ☐ Recommend paragraph _____ on page _____ be changed as follows:
(attached separate sheet if necessary)

- ☐ In a future change to this order, please include coverage on the following subject
(briefly describe what you want added):

- ☐ Other comments:

- ☐ I would like to discuss the above. Please contact me.

Submitted by: _____ Date: _____

Telephone Number: _____ Routing Symbol: _____