

**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)**

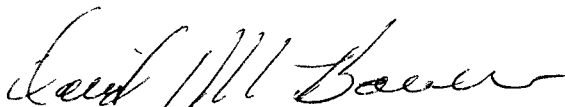
---

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 **Disposition of Transmittal Paragraph.** Retain this transmittal sheet until the directive is cancelled or superseded.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

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.