U.S. Department of Transportation

# Privacy Impact Assessment

## Federal Aviation Administration

## FAA

## Accident and Incident Data System

## AIDS


### Responsible Official

Harish Pai
Email: harish.pai@faa.gov
Phone Number: 405-954-8028

### Reviewing Official

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer
privacy@dot.gov


## Executive Summary

The Accident and Incident Data System (AIDS) is owned and operated by the Federal Aviation Administration's (FAA) Office of Aviation Safety (AVS). When an accident/incident occurs, an FAA Inspector-In-Charge (IIC) completes the FAA Form 8020-23, *FAA Accident/Incident Report* electronically within the Air Traffic Quality Assurance system (ATQA), a component of the ATO Application Portal (AAP)[1]. The FAA Form 8020-23 is then transferred from the ATQA in real-time through Transmission Control Protocol (TCP) into the AIDS. AIDS is the official repository for aviation accident and incident investigations and shares accident/incident data with various AVS systems via the AVS Replication Server.

The FAA is publishing this Privacy Impact Assessment (PIA) in accordance with the E-Government Act of 2002 because the FAA receives, uses, and maintains personally identifiable information (PII) from members of the public, specifically, pilots, flight crew, passengers and any individuals injured or deceased[2] during an aviation accident or incident. Additionally, the FAA receives, uses, and maintains PII on FAA employees and contractors.



## What is a Privacy Impact Assessment?

*The Privacy Act of 1974 articulates concepts for how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The assessment is a practical method for evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed. The PIA is an analysis of how information is handled to—i) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; ii) determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and iii) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.*[3]

*Conducting a PIA ensures compliance with laws and regulations governing privacy and demonstrates the DOT's commitment to protect the privacy of any personal information we*

[1] PIAs can be found at https://www.transportation.gov/individuals/privacy/privacy-impact-assessments.
[2] Privacy rights are not extended to the deceased; however, the FAA continues to protect and manage their PII nevertheless.
[3] Office of Management and Budget's (OMB) definition of the PIA taken from guidance on implementing the privacy provisions of the E-Government Act of 2002 (see OMB memo of M-03-22 dated September 26, 2003).

*collect, store, retrieve, use and share. It is a comprehensive analysis of how the DOT's electronic information systems and collections handle personally identifiable information (PII). The goals accomplished in completing a PIA include:*

- *Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk, and of options available for mitigating that risk;*
- *Accountability for privacy issues;*
- *Analyzing both technical and legal compliance with applicable privacy law and regulations, as well as accepted privacy policy; and*
- *Providing documentation on the flow of personal information and information requirements within DOT systems.*

*Upon reviewing the PIA, you should have a broad understanding of the risks and potential effects associated with the Department activities, processes, and systems described and approaches taken to mitigate any potential privacy risks.*



## Introduction & System Overview

The Federal Aviation Act of 1958, as amended, gives the FAA 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.

***Background***

The AIDS aviation data is used to support FAA certification and regulatory responsibilities, accident prevention programs, and to answer inquiries from the aviation industry, the media, and the public. FAA employees and contractors use AIDS as the authoritative source for all investigated, completed aviation events.

***Business Process and System Process***

Upon the occurrence of an aviation event, an FAA IIC investigates and collects information relating to the event. The IIC may review documentation, interview witnesses, collect artifacts, visit locations, and meet with other investigators in the course of their investigation. The investigative results may include PII about the individuals questioned or

investigated regarding an event including from pilots, witnesses, passengers, or ground crew as well as FAA employees and contractors.

The IIC accesses the ATQA system and manually enters information into the Form 8020-23, *FAA Accident/Incident Report* (the Report). The PII entered into the Form 8020-23 may include the name of the air operator; the pilot's full name, date of birth (DOB), residence zip code, dates and types of pilot training, date hired (if employed by an air carrier), airman certificate number and type; aircraft registration number, make, model, and serial number; FAA employees and contractors name, region/office and email address; name of witnesses, passengers and ground crew; ATQA tracking number and National Safety Transportation Board (NSTB) identity number. Additionally, the IIC may use free form text fields to enter facts or sequences of events that are relevant to the accident or incident and in doing so may enter the full names of witnesses, passengers or ground crew including those injured or deceased in the accident or incident.

Once the report is complete, the ATQA system transfers all information to AIDS in real-time through TCP. AIDS then shares accident/incident data with various AVS systems via the AVS Replication Server. Please see the Purpose Specification section in the Fair Information Practice Principles (FIPPS) Analysis for a discussion.



## Fair Information Practice Principles (FIPPs) Analysis

*The DOT PIA template is based on the fair information practice principles (FIPPs). The FIPPs, rooted in the tenets of the Privacy Act, are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs provide a framework that will support DOT efforts to appropriately identify and mitigate privacy risk. The FIPPs-based analysis conducted by DOT is predicated on the privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v3[4], sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council and the Privacy Controls articulated in Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations[5].*

## Transparency

*Sections 522a(e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act require public notice of an organization's information practices and the privacy impact of government programs and activities. Accordingly, DOT is open and transparent about*

[4] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf
[5] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf

*policies, procedures, and technologies that directly affect individuals and/or their personally identifiable information (PII). Additionally, the Department should not maintain any system of records the existence of which is not known to the public.*

DOT and FAA System of Records Notices (SORNs) provide transparency about privacy practices regarding the collection, use, sharing, safeguarding, maintenance, and disposal of information about individuals covered under the Privacy Act of 1974, as amended. The information in AIDS is covered by DOT/FAA 847, "*Aviation Records on Individuals*" 75 FR 68849 (November 9, 2010), because the information stored in the system may be retrieved by pilot names, airmen certificate numbers and aircraft registration numbers. The FAA retrieves system access records in AIDS by name and protects those Privacy Act records in accordance with Department published SORN DOT/ALL 13, "*Internet/Intranet Activity and Access Records,*" 67 FR 30757 (May 7, 2002).

The FAA may publish further notifications in the *Federal Register (FR)* to promote transparency to the public, such as: https://www.federalregister.gov/documents/2005/11/22/05-23101/faa-accident-and-incident-data-system-records-expunction-policy.

Lastly, the publication of this PIA further demonstrates transparency into AIDS and to provide notice to the public as to the information management policies and practices related to AIDS.

## Individual Participation and Redress

*DOT provides a reasonable opportunity and capability for individuals to make informed decisions about the collection, use, and disclosure of their PII. As required by the Privacy Act, individuals should be active participants in the decision-making process regarding the collection and use of their PII and they are provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.*

The sole source of AIDS records is from the ATQA system. Other than the IIC, individuals cannot access, correct, or amend their information in AIDS themselves. Any changes to AIDS records can only be accomplished by the IIC by going back through the ATQA system to amend the records and having the amended records re-transmitted to AIDS where the previous records are overwritten.

Under the provisions of the Privacy Act, individuals may request searches to determine if any records pertain to them. Individuals wishing to know if their records appear in a system may inquire in person or in writing, as follows:

**Notification Procedure (for access to records):**
Aviation Data Systems Branch, AFS-620
Federal Aviation Administration
Mike Monroney Aeronautical Center
P.O. Box 25082
6500 South MacArthur Blvd.
Oklahoma City, Oklahoma 73125

The request must include the following information:

- Full Name
- Mailing address
- Phone number and/or email address
- A description of the records sought, and if possible, the location of the records
- A statement under penalty of perjury that the requester is the individual who he or she claims to be.

**Contesting Record Procedures (for redress/amendment of records):**

An individual who wants to contest information about themselves that is contained in this system should make their request in writing, detailing the reasons for why the records should be corrected and addressing their letter to the following address:

Aviation Data Systems Branch, AFS-620
Federal Aviation Administration
Mike Monroney Aeronautical Center
P.O. Box 25082
6500 South MacArthur Blvd.
Oklahoma City, Oklahoma 73125

## Purpose Specification

*DOT should (i) identify the legal bases that authorize a particular PII collection, activity, or technology that impacts privacy; and (ii) specify the purpose(s) for which it collects, uses, maintains, or disseminates PII.*

The FAA utilizes AIDS and the information stored therein pursuant to the following legal authorities:

1) Title 49 United States Code (U.S.C.) § 40101, Policy, which covers matters relating to aviation safety;

2) Title 49 U.S.C., Transportation, Subtitle VII — Aviation Programs, PART A — Air Commerce and Safety, § 40113, which covers administrative activities with respect to security duties and powers designated to be carried out by the Under Secretary or the Administrator of the Federal Aviation Administration; and
3) Title 49 U.S.C. § 44702, Issuance of Certificates, which covers the issuance of airman certificates, design organization certificates, type certificates, production certificates, airworthiness certificates, air carrier operating certificates, airport operating certificates, air agency certificates, and air navigation facility certificates.

AIDS data will be used by the FAA consistent with the purposes for which it was collected as described in the SORNs for DOT/FAA 847, "*Aviation Records on Individuals*", 75 FR 68849 (November 9, 2010). System access data will be used by the FAA consistent with the purposes for which it was collected as described in the SORN DOT/ALL 13, "*Internet/Intranet Activity and Access Records,*" 67 FR 30757 (May 7, 2002).

AIDS is the authoritative source for all investigated, completed aviation events. The AIDS aviation data is used to support FAA certification and regulatory responsibilities, accident prevention programs, and to answer inquiries from the aviation industry, the media, and the public.

From the ATQA system, AIDS receives and maintains the following PII about the individuals questioned or investigated, regarding an event, including from pilots, witnesses, passengers, ground crew, and FAA employees or contractors. The PII may include the air operator name; pilot's full name, DOB, residence zip code, dates and types of pilot training, date hired (if employed by an air carrier), and airman certificate number and type; FAA employees and contractors name, region/office and email address; name of witnesses, passenger and ground crew; aircraft registration number, make, model, and serial number, ATQA tracking number and NSTB identity number. Additionally, the IIC may use a free form text field to enter facts or sequences of events that are relevant to the accident or incident and in doing so may enter the full names of witnesses, passengers, or ground crew injured or deceased in the accident or incident. Names of the injured or deceased may be given by witnesses, from surviving passengers or crew, or come from a passenger manifest.

AIDS internally shares accident/incident data including airmen's name, DOB and certificate number; aircraft registration number, make, model, and serial number; narrative text that could include the name of witnesses, passenger and ground crew related to the event, and date of the accident or incident with various AVS systems via the AVS Replication Server. The purpose of this data exchange is to get data to downstream systems in order to determine if a particular airman was involved in a prior accident or incident or to further

investigate aircraft parts safety and provide analysis to address safety issues regarding aircraft. The following systems receive this data:

- Accident Incident Enforcement (AIE),
- Enforcement Information System Query and Browse (EISQB)
- Pilots Records Database (PRD)
- Safety Performance Analysis System (SPAS),
- Monitor Safety Analyze Data (MSAD),
- Enterprise Information Management (EIM) Platform,
- Safety Assurance System (SAS),
- Aviation Safety Information Analysis and Sharing (ASIAS)

From the FAA Directory Service, AIDS receives the email address, and it is used to authenticate all FAA employees and contractors into the system.

Currently, there is no external sharing of recent AIDS data. However, in the past, for transparency, the FAA provided limited data from AIDS to the public via the FAA website https://www.faa.gov/data_research/accident_incident/. All PII was removed prior to publication. However, FAA no longer posts AIDS data to any public website, including this one.

## Data Minimization & Retention

*DOT should collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected.*

The FAA minimizes its data maintenance, use, and retention in AIDS to the information that is relevant and necessary to meet its authorized business purpose, which is to evaluate the facts surrounding an event and mitigate the risk of a repeated occurrence.

The FAA submitted a new records retention and disposition schedule, DAA-0237-2021-011, to the National archives and Records Administration (NARA) in which it proposes to maintain Accident and Investigation Reports for 99 years and Pilot Information until notification of the pilot's death or when the pilot reaches 99 years of age. The FAA will retain records in this system of records as permanent records until it receives approval of record disposition authority from NARA.

System access records are governed by NARA General Records Schedule (GRS) 3.2, approved September 2016, Information Systems Security Records. Under that schedule, system access records are destroyed when business use ceases.

## Use Limitation

*DOT shall limit the scope of its PII use to ensure that the Department does not use PII in any manner that is not specified in notices, incompatible with the specified purposes for which the information was collected, or for any purpose not otherwise permitted by law.*

DOT discloses AIDS information outside DOT in accordance with DOT/FAA 847, "*Aviation Records on Individuals,*" 75 FR 68849 (November 9, 2010). In addition to other disclosures generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act, all or a portion of the records or information contained in AIDS may be disclosed outside DOT as a routine use pursuant to 5 U.S.C. § 552a(b)(3) to:

- Disclose information to the NTSB in connection with its investigation responsibilities.
- Provide information about airmen to Federal, State, local and Tribal law enforcement agencies when engaged in an official investigation in which an airman is involved.
- Make airman, aircraft and operator record elements available to agencies relating to aviation events including the Department of Defense, the Department of Homeland Security, the Department of Justice and other authorized government users, for their use in managing, tracking and reporting aviation-related security events.

The sharing of user account information in the AIDS system is conducted in accordance with SORN DOT/ALL 13, "*Internet/Intranet Activity and Access Records*", 67 FR 30758 ( May 7, 2002). In addition to other disclosures generally permitted under 5 U.S.C. §552(a)(b) of the Privacy Act, all or a portion of the records or information contained in the system may be disclosed outside DOT as a routine use pursuant to 5 U.S.C § 552a(b)(3) as follows:

• To provide information to any person(s) authorized to assist in an approved investigation of improper access or usage of DOT computer systems.

• To an actual or potential party or his or her authorized representative for the purpose of negotiation or discussion of such matters as settlement of the case or matter, or informal discovery proceedings.

• To contractors, grantees, experts, consultants, detailees, and other non-DOT employees performing or working on a contract, service, grant cooperative agreement, or other assignment from the Federal government, when necessary to accomplish an agency function related to this system of records.

• To other government agencies where required by law.

DOT may also disclose AIDS information outside DOT pursuant to 15 additional routine uses applicable to all DOT Privacy Act systems of records. These routine uses are published

in the *Federal Register* at 75 FR 82132 (December 29, 2010), and 77 FR 42796 (July 20, 2012).

## Data Quality and Integrity

*In accordance with Section 552a(e)(2) of the Privacy Act of 1974, DOT should ensure that any PII collected and maintained by the organization is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in the Department's public notice(s).*

AIDS receives information from the ATQA system and does not collect information directly from an individual. If there are any changes that need to occur to the Report data collected during or after the investigative process, the IIC must initiate those changes in the ATQA system, where the data would be amended and then re-transferred to AIDS.

During the file transfer from ATQA, there is no human interface which eliminates the possibility of human error possibly impacting the quality of the data.

Further, AIDS does not allow a user (other than for the application administrator) to add, delete or revise information and PII within AIDS, which helps preserve data quality and greatly reduces the opportunity for the quality or integrity of the data to be compromised.

## Security

*DOT shall implement administrative, technical, and physical measures to protect PII collected or maintained by the Department against loss, unauthorized access, or disclosure, as required by the Privacy Act, and to ensure that organizational planning and responses to privacy incidents comply with OMB policies and guidance.*

FAA protects PII with reasonable security safeguards against loss or unauthorized access, destruction, usage, modification, or disclosure. These safeguards incorporate standards and practices required for federal information systems under the Federal Information Security Management Act (FISMA) and are detailed in Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information Systems, dated March 2006, and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, dated April 2013.

AIDS employs specific administrative, technical, and physical measures to protect PII against loss, unauthorized access, or disclosure. Personnel can only access the internal interfaces via FAA's network using their Personal Identity Verification (PIV) card. All PII is encrypted in transit and at rest. Personnel receive guidance on their duties as they relate to

collecting, using, processing, and securing PII. This includes mandatory annual security and privacy awareness training, as well as a review of the FAA Rules of Behavior. The DOT and FAA Privacy Office conduct periodic privacy compliance reviews of AIDS, as related to the requirements of OMB Circular A-130, Managing Information as a Strategic Resource.

A limited number of AVS personnel have access to an AIDS internal interface that displays all its PII. Each has a business need to access AIDS, such as the individual responsible for assuring that the ATQA system correctly transfers information into AIDS. Once given access, they may view all the information obtained from the database and create metrics from that information.

AIDS has in place a privacy/security incident response plan which includes procedures for detection of a privacy/security incident, remediation and response if one occurs, and notification where appropriate to protect and inform impacted individuals. In addition, the AIDS administrators, privacy personnel, and security personnel have conducted a privacy/security incident response exercise to evaluate the effectiveness of this plan.

AIDS has a system security plan in place. The system was issued an Authority to Operate on August 5, 2020, after completing the authorization and accreditation process that reviews security controls and procedures and that validates that AIDS is compliant with appropriate information security processes and policies.

## Accountability and Auditing

*DOT shall implement effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that the Department is complying with all applicable privacy protection requirements and minimizing the privacy risk to individuals.*

FAA Order 1370.121B, FAA Information Security and Privacy Program & Policy, implements the various privacy requirements of the Privacy Act of 1974 (the Privacy Act), the E-Government Act of 2002 (Public Law 107-347), DOT privacy regulations, Office of Management and Budget (OMB) mandates, and other applicable DOT and FAA information and information technology management procedures and guidance.

In addition to these practices, the FAA will implement additional policies and procedures as they relate to the access, protection, retention, and destruction of PII. Federal employees and contractors who work with AIDS are given clear guidance about their duties as related to collecting, using, and processing privacy data. Guidance is provided in mandatory annual security and privacy awareness training, as well as FAA Order 1370.121B. As previously stated, the FAA will conduct periodic privacy compliance reviews of the AIDS as related to the requirements of OMB Circular A-130, Managing Information as a Strategic Resource.

## Responsible Official

Harish Pai
System Owner
ADE-540, Office of Information & Technology (AIT)

Prepared by: Barbara Stance, FAA Privacy Officer

## Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer