U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration (FAA)

Office of Aviation Safety (AVS)

Responsible Official

Sherry Christeson
Email: sherry.christeson@faa.gov

Reviewing Official

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

Executive Summary

The Office of Aviation Safety (AVS) Hub is the Federal Aviation Administration's (FAA) single sign-on platform for certificated individuals, unmanned aircraft system (UAS) operators, business entities and manufacturers who interact with the FAA to apply for or submit requests for a variety of certificates, waivers, and approvals under a variety of Parts pursuant to the Federal Aviation Regulations (FAR). The AVS Hub is hosted on the Pega Platform, which is a subsystem of the FAA's Robotic Process Automation Environment (FRAME).

In accordance with the E-Government Act of 2002, the FAA developed this Privacy Impact Assessment (PIA) because AVS Hub collects Personally Identifiable Information (PII) on members of the public, such as individual UAS Operators, business entities, and manufacturers. This PIA covers account creation and authentication within AVS Hub only. The workflows available via the AVS Hub are discussed in the applicable PIA appendices to this PIA and can be found on the Department of Transportation's PIA page. Additional workflows will be added to AVS Hub in the future, and if required, a PIA appendix will be added to this document to address all privacy concerns for individual services.

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.[1]

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 collect, store, retrieve, use and share. It is a comprehensive analysis of how the DOT's

[1]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).

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 Office of Aviation Safety (AVS) Hub was developed pursuant to 49 U.S.C. 322, General Powers, and 49 U.S.C. 40101, and under 49 U.S.C. Subtitle 106, to host multiple workflows for a variety of UAS services that are required under different legal authorities (see Appendices for each workflow and corresponding legal authority).

The application is accessible to FAA employees/contractors and members of the public. FAA employees navigate to the internal workspace on aviationsafetyinternalportal.faa.gov and authenticate via MyAccess using their personal Identity Verification (PIV) card.

Members of the public are required to create a MyAccess account for access to the system. To create an account via MyAccess, the external user is redirected from the AVS Hub to a MyAccess page with options for creating credentials. The MyAccess PIA has further details on how identity verification occurs via login.gov. Once the individual has a MyAccess credential, they can access AVS Hub.

Within AVS Hub, the external user creates a profile with the following information, depending on the user's purpose for accessing the system:

- If they are an individual UAS operator, the following PII is manually input: name, physical address, email address, and phone number.
- If they are a representative of a business, the following PII is manually input: representative name, job title, country, business name, business name, business email address, business address, and business phone number.

Once the external user has created their profile, they can access the applicable workflow to complete their application or request. After authentication, AVS Hub performs authorization

and role assignment within the application to determine user permissions. External users also have the opportunity to review a Privacy Act Statement before providing their PII.

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[2], 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[3].

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 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.

The FAA deploys multiple techniques to ensure that individuals are informed of the purpose for which the FAA collects, uses, disseminates, and retains PII within the AVS Hub. AVS Hub maintains records on stakeholders, which are retrievable by unique identifiers. Please see the associated PIA appendices for further explanation of each AVS Hub workflow.

The Department of Transportation (DOT) has published the following Privacy Act System of Records Notice (SORN), providing notice to the public of its privacy practices regarding the collection, use, sharing, safeguarding, maintenance, and disposal of information about an individual that may be collected in the account creation and authentication process that is covered herewith.

Records are subject DOT/ALL 13, Internet/Intranet Activity and Access Records, 67 FR 30757 (May 7, 2002) which provides notice to stakeholders of records of system access.

This SORN addresses only the information collected during account creation and does not cover the AVS Hub workflows. Applicable AVS Hub workflows are covered by a Privacy

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

Act notice specific to that service and are identified as part of the application in its specific PIA appendix associated with this document.

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 with reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

All information within AVS Hub is voluntarily collected from the stakeholders. Please see the PIA appendices for the specific AVS Hub services that address the collection, use, and disclosure of PII in applicable workflows.

Under the Privacy Act, individuals may request searches to determine whether any records that may pertain to them have been added. Individuals wishing to know if their records appear in this system may inquire in person or in writing to:

Federal Aviation Administration

Privacy Office

800 Independence Ave., SW

Washington, District of Columbia (DC) 20591

Included in the request must be the following:

• Name
• Mailing address
• Phone number and/or e-mail address
• A description of the records sought, and if possible, the location of the records

Contesting record procedures: Individuals wanting to contest information about themselves that is contained in this system should make their requests in writing, detailing the reasons why the records should be corrected to the following address:

Federal Aviation Administration
Privacy Office
800 Independence Ave. SW
Washington DC, 20591

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 PII contained in PTB is utilized for transit subsidy u

PII data in the system of records (account information, including name, personal/business email address, personal/business phone number, job title, business name, and address) is used by DOT systems and security personnel or persons authorized to assist these personnel, to plan and manage systems services and otherwise perform their official duties. Such services would include, but are not limited to, analyzing engineering and statistical usage data to assist in making business decisions regarding upgrading hardware, software, and communications technology to meet changing Internet/Intranet usage requirements. The system is also used to monitor for improper use.

Specific legal authorities for each AVS Hub workflow are cited in the applicable appendices to this PIA.

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.

Individuals creating accounts in AVS Hub are responsible for the accuracy of the information they provide during the process. The personal information collected for account registration is the minimum required to establish unique accounts within the system, ensure appropriate access to services, and maintain communications with registered individuals.

The AVS Hub account information are retained and disposed of in accordance with National Archives and Records Administration, General Records Schedule (GRS) 3.2, Information Systems Security Records, Item 030: System Access Records. An individual's system access records are maintained in AVS Hub as temporary records and are destroyed when business use ceases. Please see the associated PIA appendices for a full discussion of the minimization and retention policy for records related to the individual AVS Hub workflows.

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.

The sharing of AVS Hub account registration and user activity logs in AVS Hub is conducted in accordance with Department 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. § 552a(b) of the Privacy Act, all or a portion of the records or information contained in this 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.

The Department has also published 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, under ‘‘Prefatory Statement of General Routine Uses.” The Sharing of Privacy Act records collected, used, and maintained as part of the back-end services are discussed in the associated appendices for the back-end services.

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).

Registrants are responsible for ensuring the accuracy of their authentication information when creating their MyAccess credentials and profile. Once the user profile is complete, individuals can log in to the system and update their PII as needed. The data quality and integrity needs of the AVS Hub workflows are discussed in the applicable PIA appendices.

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.

The 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.

AVS Hub has a built-in time-out function, and stakeholders are automatically logged out after 60 minutes of inactivity. In addition, all AVS Hub workflows securely transmit information provided by the stakeholders using third-party authentication services, which protect the data using Hypertext Transfer Protocol encrypted by Transport Layer Security/Secure Sockets Layer. AVS Hub is hosted on the Pega Platform, which is a Federal Risk and Authorization Management Program Compliant Cloud Service Provider, meeting Moderate Federal Risk and Authorization Management Program security requirements.

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 implements the various privacy requirements of the Privacy Act of 1974 (the Privacy Act), the E-Government Act of 2002 (Public Law 107-347), the FISMA, DOT privacy regulations including DOT Privacy Risk Management Policy Order 1351.18, 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, additional policies and procedures are consistently applied, especially as they relate to access, protection, retention, and destruction of PII. Federal and contract employees are given clear guidance on their duties related to collecting, using, and processing privacy data. Guidance is provided through mandatory annual security and privacy awareness training and FAA Order 1370.12.1B. The FAA conducts periodic privacy compliance reviews of the AVS Hub relative to the requirements of OMB Circular A-130.

Responsible Official

Sherry Christeson, System Owner

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Digital & Information Officer

KARYN MARIE GORMAN
Digitally signed by KARYN MARIE GORMAN
Date: 2026.05.29 10:08:07 -04'00'