



U.S. Department of Transportation
Privacy Impact Assessment
Federal Aviation Administration (FAA)

U.S. Agents for Service Portal
USAS

Responsible Official

Kelly Merritt
Email: Kelly.A.Merritt@faa.gov
Phone Number: 405.954.3815

Reviewing Official

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





Executive Summary

The Federal Aviation Administration (FAA) developed the U.S. Agent for Service (USAS) Portal to implement the “[U.S. Agents for Service on Individuals With Foreign Addresses Who Hold or Apply for Certain Certificates, Ratings, or Authorizations](#)” final rule. The FAA requires individuals with foreign addresses and no physical address in the U.S. on file to designate a U.S. Agent who can receive FAA documents on their behalf. The designated U.S. Agent helps ensure the timely and cost-effective delivery of important FAA documents, facilitating the prompt service of process and other time-sensitive communications for individuals. The designated U.S. Agent can be an individual or a Service Agent company. For the purposes of this Privacy Impact Assessment (PIA), the designated U.S. Agent is referred to as Individuals.

The FAA is publishing this PIA in accordance with Section 208 of the [E-Government Act of 2002](#) because the USAS Portal collects Personally Identifiable Information (PII) about individuals designated as U.S. Agent.

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 electronic information systems and collections handle personally identifiable information (PII). The goals accomplished in completing a PIA include:

¹Office 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).



- *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 within the FAA developed the USAS Portal to implement the final rule for [“U.S. Agents for Service on Individuals With Foreign Addresses Who Hold or Apply for Certain Certificates, Ratings, or Authorizations.”](#) Individuals who hold or apply for certificates issued under [14 CFR parts 47, 61, 63, 65, 67, or 107](#) and do not have a U.S. physical address of record on file with the FAA must designate a U.S. Agent for service.

Individuals around the world can apply for and obtain FAA certificates, ratings, and authorizations. However, serving certain documents to these individuals poses a challenge for the FAA. Establishing service of process abroad requires adherence to international service requirements under multilateral treaties and applicable U.S. laws regulating extraterritorial service. The USAS Portal enables Individuals with foreign addresses and no physical address in the U.S. on file to designate a U.S. Agent for service to receive important documents on their behalf.

With the deployment of the USAS Portal, when individuals navigate to the Civil Aviation Registry Applications (AVS Registry), Integrated Airman Certification and Rating Application (IACRA) or Medical Support System (MSS), they receive a notice to designate a U.S. Agent. Individuals that do not have a U.S. physical address of record on file or have not designated a U.S. Agent must navigate to the USAS Portal to designate a U.S. Agent.

The USAS Portal receives a one-time data extraction from the following FAA systems to pre-populate the USAS Portal.

- The AVS Registry System² sends the name, email address, N-number and serial number for aircraft records and the name, email address, FAA Tracking Number (FTN), and date of birth (DOB) for airmen certification records.

² The PIA for AVS Registry System is available at [Privacy Impact Assessment - FAA Aircraft Registration System and Airmen Certification System | US Department of Transportation](#)



- MSS³ sends the name, email address, FTN and DOB for medical certification records.

System Access

Individuals navigate to <https://usas.faa.gov> to create a user account for the USAS Portal. During the registration process, they must enter their name, email address, and select three security questions along with their answers, which may contain PII and account passwords. FAA employees log in to the USAS Portal using their Personal Identity Verification (PIV) card.

Typical Transaction

Individuals can log into the USAS Portal based on whether they hold a medical certificate, airmen certificate, or aircraft registration. The individual must provide specific information based on their category.

- Individuals with a medical or airmen certificate enter their FTN and DOB.
- Individuals with an aircraft registration enter their aircraft N-number and serial number.

In all cases, the USAS Portal searches its database to determine if the individual has a designated U.S. Agent on file. If a U.S. Agent exists, the individual can make changes as needed. If no U.S. Agent is on file, the individual must enter the following PII for the U.S. Agent: name, address, optional phone number, optional fax number, and email address. The individual U.S. Agent must first check a box to indicate whether the U.S. Agent is a military employee registering on behalf of the Department of Defense.

Additionally, if the individual is registering as a Service Agent company as the U.S. agent, the individual must provide the company name, address, optional phone number, optional fax number, and email address. The Service Agent representative details are optional but include the first name, middle name, last name, suffix, phone number, optional fax, and email address.

The USAS Portal then verifies the individual U.S. Agent and/or the Service Agent company address using the SMARTY STREETS address verification service. SMARTY STREETS address verification service can standardize addresses, verify address accuracy, provide suggestions for correcting addresses that aren't recognized, and indicate if an address is a valid delivery point to confirm that the address is accurate and a U.S. address.

³ The PIA for Medical Support System is available at [Medical Support Systems \(MSS\) | US Department of Transportation](#)



After entering the designated U.S. Agent information, the individual designating a U.S. Agent or using a Service Agent company selects a check box confirming the U.S. Agent is aware of their responsibility to promptly transmit documents on their behalf. Once the information is submitted, a success message appears informing the individual the U.S. Agent and Service Agent company information was saved successfully. Individuals can access the USAS Portal to edit or update their U.S. Agent designation when needed.

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, 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.

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 uses several methods to inform individuals about its information collection and usage practices. One such method is publishing the final rule titled [U.S. Agents for Service on Individuals With Foreign Addresses Who Hold or Apply for Certain Certificates, Ratings, or Authorizations](#) as a means of notice. In addition, a Privacy Act Statement (PAS) and a Paperwork Reduction Act (PRA) Statement on the USAS Portal's landing page provide notice of information collected for system access and information collected from the public.

The Department of Transportation (DOT) and FAA System of Record 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 collected is covered by:

- [DOT/FAA 801 Aviation Registration Records, August 9, 2023, 88 FR 53951](#)



- [DOT/FAA 847 – Aviation Records on Individuals June 10, 2024, 89 FR](#)
- [DOT/ALL 13, Internet/Intranet Activity and Access Records, 7, 2002, 67 FR 30757](#)

The publication of this PIA demonstrates DOT’s commitment to provide appropriate transparency into the USAS Portal process to designate a U.S. Agent for service.

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.

Individuals who hold a medical certificate, airmen certificate, or aircraft registration enter information about their designated U.S. Agents. Throughout the process, individuals can edit and update the designated U.S. Agent information through the USAS Portal.

Under the provisions of the Privacy Act, individuals may request a search of the USAS Portal to determine if any records may pertain to them. Individuals wanting copies of records about themselves stored in this system should make their requests in writing, explaining that they want copies of the records require correction to the following address:

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

The following must be included in the request:

- Name
- Mailing Address,
- Phone number or email address,
- A description of the records sought, and if possible, the location of records.

Individuals requesting correction of their records in the USAS Portal database should make their requests in writing, detailing the reasons why the records need correction to the following address:

Federal Aviation Administration
Privacy Office
800 Independence Ave. SW



Washington DC, 20591

Additional information about the Department’s privacy program may be found at www.transportation.gov/privacy. Individuals may also contact the DOT Chief Privacy Officer at privacy@dot.gov.

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 usage reconciliation, reporting for the agency, monitoring, and tracking participant usage.

The FAA developed the USAS Portal to implement a final rule for “[U.S. Agents for Service on Individuals With Foreign Addresses Who Hold or Apply for Certain Certificates, Ratings, or Authorizations](#)”. Individuals who hold or apply for certificates issued under [14 CFR parts 47, 61, 63, 65, 67, or 107](#) and do not have a U.S. physical address of record on file with the FAA must designate a U.S. Agent for service.

The USAS Portal sends or receives the following information to or from other FAA systems:

- AVS Registry System sends a one-time data exchange to pre-populate the USAS Portal which includes: the name, email, N- number and serial number for Aircraft Records and the name, email, FTN and DOB for airmen certification Records.
- MSS sends a one-time data exchange which includes: the name, email, FTN and DOB for medical certification records.
- Document Imaging Workflow System (DIWS)/MSS receives from the USAS Portal: the U.S. Agent’s name, address, phone number and email address. The USAS Portal connects to the DIWS application to ensure the secure transfer of the airmen’s data, which is U.S. Agent information. This data is stored within the DIWS application.
- MyAccess receives FAA employees’ and contractors’ business email address. That information is used for authenticating and providing access to the USAS Portal.

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 USAS Portal collects the minimum amount of information to reduce the privacy risks associated with the project.



The USAS Portal does not have an approved records retention schedule from the National Archives and Record Administration (NARA). FAA is proposing to maintain the record for 5 years. Records for the USAS Portal will be maintained as permanent records until the FAA receives an approved disposition authority from NARA.

System access records are maintained in accordance with [NARA General Records Schedule \(GRS\) 3.2, Information Systems Security Records](#), approved January 2, 2023 and 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.

The USAS Portal shares the entered address with SMARTY STREET to verify the designated U.S. Agent's address. The FAA and SMARTY STREET have a service provider agreement that governs the sharing of PII and the use of that information. The FAA discloses information in the USAS Portal in accordance with the following Department published System of Record Notices.

The FAA discloses aircraft records with designated U.S. Agent on file information in accordance with [DOT/FAA 801 Aviation Registration Records, August 9, 2023, 88 FR 53951](#). 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 USAS Portal may be disclosed outside DOT as a routine use pursuant to 5 U.S.C. § 552a(b)(3) to:

- To law enforcement, when necessary and relevant to an FAA enforcement activity.
- To government agencies, whether Federal, State, Tribal, local, or foreign, information necessary or relevant to an investigation of a violation or potential violation of law, whether civil, criminal, or regulatory, that the agency is charged with investigating or enforcing; as well as, to government agencies, whether Federal, State, or local responsible for threat detection in connection with critical infrastructure protection.

FAA discloses airmen certification records with designated U.S. Agent on file information in accordance with [DOT/FAA 847 – Aviation Records on Individuals June 10, 2024, 89 FR](#). 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 USAS Portal may be disclosed outside DOT as a routine use pursuant to 5 U.S.C. § 552a(b)(3) to:



- Disclose information to the National Transportation Safety Board (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.
- Provide information about airmen to Federal, State, local, and Tribal law enforcement, national security, or homeland security agencies whenever such agencies are engaged in the performance of threat assessments affecting the safety of transportation or national security.

The sharing of user account information in the USAS Portal is conducted in accordance with SORN [DOT/ALL 13, Internet/Intranet Activity and Access Records 7, 2002, 67 FR 30757](#).

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 the USAS Portal 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 \(December 29, 2010\)](#), [77 FR 42796 \(July 20, 2012\)](#), and [84 FR 55222 \(October 15, 2019\)](#).

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).

The FAA collects and retains the relevant and necessary information for the purposes it was collected. The USAS Portal receives a one-time data exchange from the AVS Registry and MSS to pre-populate the USAS Portal. The AVS Registry System provides the name, email, N-number and serial number for aircraft records. MSS sends the name, email address, and DOB for the airman certification record. Individuals holding a medical certificate, airmen certificate, or an aircraft registration enter information about the U.S. Agent they designate



and are responsible for ensuring the accuracy of the information they enter. In all instances, the individual can access the system as needed to make changes as necessary.

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 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 5, Security and Privacy Controls for Federal Information Systems and Organizations, dated September 2020 (includes updates as of Dec. 10, 2020).

The USAS Portal implements a combination of administrative, technical, and physical measures to protect PII from loss, unauthorized access, or disclosure. To safeguard PII, the USAS Portal takes the following steps: identification and authentication, physical security, user roles and permissions, and encryption. FAA employees can access the internal interface only through the FAA's network using their PIV cards. All PII is encrypted both in transit and at rest. FAA employees receive guidance on their responsibilities related to the collection, use, processing, and security of PII, which includes annual security and privacy awareness training and a review of the FAA Rules of Behavior.

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 the USAS Portal 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. The FAA will conduct periodic privacy compliance reviews of the USAS Portal as related to the requirements of OMB Circular A-130, Managing Information as a Strategic Resource.

Responsible Official

Kelly Merritt
Program Manager
AVS/FAA

Prepared by: Barbara Stance, FAA Privacy Officer

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

DOT Privacy Office - Approved - 04/04/2025