



**U.S. Department of Transportation**

## **Privacy Impact Assessment**

**Federal Aviation Administration**

**FAA**

### **Office of Aviation Safety Voluntary Safety Reporting Program System**

#### **AVS VSRP**

##### **Responsible Official**

Robert P. Huber

Email: [VSRP@FAA.gov](mailto:VSRP@FAA.gov)

Phone Number: 877-480-4354

##### **Reviewing Official**

Karyn Gorman,

Chief Privacy Officer

Office of the Chief Information Officer

[privacy@dot.gov](mailto:privacy@dot.gov)





## Executive Summary

The Federal Aviation Administration Office (FAA) of Aviation Safety (AVS) sets, oversees, and enforces safety standards for all parts of the aviation industry, impacting every facet of domestic and international civil aviation safety. AVS is responsible for the certification, production approval, and continued airworthiness of aircraft as well as the certification of pilots, mechanics, and others in safety-related positions. AVS developed the AVS Voluntary Safety Reporting Program (VSRP) to work in parallel with its safety culture to address safety concerns and to increase awareness of aviation-safety-related issues. The AVS VSRP, which is detailed in [FAA Order VS 8000.375](#) (“AVS Voluntary Safety Reporting Program”), is an online reporting tool used by AVS employees to confidentially and without punitive action or fear of reprisal report these issues that may exist across all areas of AVS. The AVS VSRP was developed under the authority of the [Federal Aircraft Certification, Safety, and Accountability Act of 2020](#).

The FAA developed this Privacy Impact Assessment (PIA) in accordance with the [E-Government Act of 2002](#) because the AVS VSRP collects Personally Identifiable Information (PII) such as name, email address, phone number and position/role from AVS employees. In addition, AVS employees enter information about an aviation-safety-related concern at their discretion. When filing an AVS VSRP report, AVS employees may also enter names, contact information and certificate numbers, etc. of members of the public if such information is relevant to the aviation-safety-related concern.

### 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.<sup>1</sup>*

*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:*

- 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 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.

---

<sup>1</sup>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).



The AVS VSRP was established on April 5, 2021, to enable AVS employees across all areas of AVS to confidentially report issues related to aviation safety without punitive action or fear of reprisal. The AVS VSRP process allows for the collection and redaction of safety data, tracking the status of ongoing investigations and any corresponding corrective actions, and helps to identify any potential systemic aviation safety hazards. The program provides for the proactive identification and mitigation of safety issues through:

- Open reporting of aviation safety issues and concerns.
- A voluntary, cooperative, confidential, and non-punitive reporting environment.
- A systematic documented review of safety concerns raised by AVS employees.
- Risk-based, data-driven development of corrective actions to mitigate identified safety concerns and systematic issues.

AVS VSRP is an internal system that is used by AVS employees and is not accessible to the public. To file an AVS VSRP report, AVS employees must navigate to <https://avsvsrp.aero/> and access the AVS VSRP using their Personal Identity Verification (PIV) card<sup>2</sup>. When submitting an AVS VSRP report, AVS employees have the option to remain anonymous. If AVS employees choose not to remain anonymous, they enter the following information on the AVS VSRP Form:

- Reporter's Name
- Reporter's FAA Email address
- Reporter's Phone Number
- Reporter's Preferred Method of Contact (*optional*)
- Reporter's Position/Role
- Date safety issue occurred (*if applicable*)
- Issue Severity (*optional*)
- Issue Likelihood (*optional*)
- Issue Category (*optional*)

The AVS employee then enters a description of the aviation safety-related issue into an open text field. In doing so, the reporting AVS employee may, at their discretion, include their name, contact information, certification numbers, and other information about members of the public that is obtained while conducting a safety inspection or during their normal daily duties and operations. In addition, the AVS employee may include attachments which could be forms, photos, certificates, or applications which may include PII such as names, individuals' contact information, and certificate numbers. The AVS employee then submits

---

<sup>2</sup>MyAccess sends the username, which is their email address, to the AVS VSRP for access and authentication purposes. See the MyAccess PIA published at <https://www.transportation.gov/individuals/privacy/myaccess-electronic-identity-authentication>.



the report and the AVS VSRP generates a submission number that is used to track and search for the report.

The AVS VSRP automatically assigns the report to an analyst for review. The analyst reviews the submission and creates a confidential report. To do so, the analyst removes the following information:

- All PII of the reporter.
- Any names or initials. All descriptions of safety concerns are put into third person (them, they, their).
- Date and time.
- Any facility names, organization/routing symbols, airline names, flight numbers or routes, and any other identifying information if it can be used to identify a submitter.

All attachments are also redacted in the same manner outlined above for all PII. Once redacted, the AVS VSRP sends the redacted report to the Event Review Team (ERT) to determine if there are any aviation-safety-related concerns that might require corrective action. If the subject of the report is deemed not to be a safety issue or if the report is not accepted, the submitter is advised that is not a safety issue, and the report is closed. If it is determined there is a safety concern, the ERT conducts an investigation. The investigation is conducted outside of the AVS VSRP; however, annotations of the investigation are made in the AVS VSRP. In most instances, the annotation would not include PII. Once the ERT completes the investigation, a Corrective Action Request is issued that identifies steps to resolve any safety concerns<sup>3</sup> and the report is closed. Reports that are not accepted are removed from the reporting tool as described in the AVS VSRP Administration Manual and Standard Operating Procedures.

Except for reports that were submitted anonymously, reporting AVS employees receive automated status updates from the system.

### **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.*

---

<sup>3</sup> Resolution can include training which is done outside of the AVS VSRP. Follow up action are taken to ensure the recommended corrective actions are completed.



*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<sup>4</sup>, 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<sup>5</sup>.*

## **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.*

Name, FAA email address, FAA phone number, and FAA position/role is collected directly from the AVS employee. When reporting an aviation-safety-related concern, the reporting AVS employee may also enter information about a member of the public. Information about a member of the public may include the individual's name, contact information and certificate number, etc. In these instances, since information is not collected directly from the individual, notice is not provided. The AVS VSRP is not searchable by the name or contact information of either the AVS employee or by any information of any members of the public. Typically, all PII pertaining to a member of the public is redacted. AVS VSRP is only searchable by the submission number or by report subject (e.g., UAS). Accordingly, VSRP is not a privacy act system of records.

The FAA provides notice of its collection, use, and disclosure of PII within this system via the publication of this PIA.

## **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.*

When submitting an AVS VSRP report, AVS employees provide their name, email address, phone number, and position/role. In some instances, the reporting AVS employee may also provide the name, contact information and certificate number etc.,

<sup>4</sup> <http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf>

<sup>5</sup> [http://csrc.nist.gov/publications/drafts/800-53-Appendix-J/IPDraft\\_800-53-privacy-appendix-J.pdf](http://csrc.nist.gov/publications/drafts/800-53-Appendix-J/IPDraft_800-53-privacy-appendix-J.pdf)





of members of the public when this information could apply to a potential aviation-safety-related issue. Once the AVS VSRP form is submitted, a submission number is generated and all PII is redacted therefore would not be able to correct amend or delete records once submitted.

### **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 [Federal Aircraft Certification, Safety, and Accountability Act of 2020](#) is the legal authority that authorizes the FAA to collect the name, email address, phone number and position/title from AVS employees that confidentially report issues related to aviation safety. Additional names, contact information, certificate numbers, etc., which may have been obtained by the AVS employee while conducting an inspection or during their normal daily duties and operations, may also be included in the report and used for resolution of the safety concern.

The AVS VSRP receives from MyAccess the user's name (which is their email address) for authentication and access.

### **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 manages privacy risk by collecting only the minimum amount of PII necessary to process accepted AVS VSRP reports of aviation-safety-related concerns. All information is submitted via the online AVS VSRP form. The form provides a standardized way for AVS employees to submit information necessary for the AVS VSRP to investigate the safety concern. Using this form limits the chance of an AVS employee submitting unnecessary or irrelevant PII to the FAA. The AVS VSRP records are maintained in accordance with record National Archives and Records Administration (NARA) disposition authority DAA-0237-2020-0028, approved on April 7, 2022. Records pertaining to accepted AVS VSRP reports are destroyed 15 years after all associated activities are complete. Reports that are not accepted in the AVS VSRP are not stored in the AVS VSRP and are deleted once they are reviewed.

### **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.*



VSRP is not a privacy act system of records. When submitting an AVS VSRP report, AVS employees can enter information about themselves as well as information about members of the public that is obtained while conducting a safety inspection; however, the focus is on fixing the safety concern and not an individual. PII pertaining to a AVS employees and member of the public is redacted and does not get shared.

### **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 AVS VSRP collects information directly from AVS employees who complete the online AVS VSRP form. AVS employees are responsible for the accuracy of the information they submit. Once the AVS VSRP form is submitted, a submission number is generated and all PII is redacted. At this point, a submitter cannot make changes. However, annotations of the investigation are made in the AVS VSRP to ensure information about the safety concern is accurate.

### **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 AVS VSRP protects PII with security safeguards against loss or unauthorized access, destruction, usage, modification, or disclosure. These safeguards incorporate standards and practices required for federal information systems in a manner consistent with applicable law and policies, including, but not limited to, the Federal Information Security Modernization Act (FISMA) 2014, Office of Management and Budget (OMB) [Circular A-130, Managing Information as a Strategic Resource](#), and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*.

### **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, as amended, 5 U.S.C. § 552a](#), the [E-Government Act of 2002 \(Public Law 107-347\)](#),





the [Federal Information Security Modernization Act \(FISMA\)](#), Pub. L. 113-283 (Dec. 18, 2014), DOT privacy regulations (including [DOT Privacy Risk Management Policy Order 1351.18](#)), 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 will be consistently applied, especially as they relate to access, protection, retention, and destruction of PII. Federal and contract employees are given clear guidance in their duties as they relate to collecting, using, and processing privacy data. Guidance is provided in the form of mandatory annual security and privacy awareness training, as well as in FAA Order 1370.121B. The FAA will conduct periodic privacy compliance reviews of the AVS VSRP services relative to the requirements of [OMB Circular A-130](#).

### **Responsible Official**

Robert P. Huber  
Email: [VSRP@FAA.gov](mailto:VSRP@FAA.gov)  
Phone Number: 877-480-4354

Prepared by: Barbara Stance, FAA Chief Privacy Officer

### **Approval and Signature**

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