



U.S. Department of Transportation

**Privacy Impact Assessment
Federal Aviation Administration (FAA)
Office of Aviation Safety (AVS)
Safety Performance Analysis System (SPAS)**

Responsible Official

Lai Lee-Birman

SPAS System Owner 9-AWA-AFS-900-SASO@faa.gov

Office of Solutions Delivery 1 (866) 835-5322

Reviewing Official

Karyn Gorman

Chief Privacy Officer

Office of the Chief Information Officer

privacy@dot.gov





Executive Summary

In support of the Federal Aviation Administration (FAA's) overall safety posture, the Safety Analysis Performance System (SPAS) provides an automated, read-only, web-based user interface for FAA employees and contractors, managers and flight coordinators, and Department of Defense (DoD) flight inspectors to query summarized and detailed data from multiple FAA systems. SPAS was developed by the FAA Aviation Safety (AVS) Organization to meet a requirement in [USC Title 49, Subtitle VII, Part A, subpart iii, Chapter 447, 44713e](#). Legal authority to maintain data in SPAS is covered under [49 U.S.C. 40101, 40113, 44701–44703, 44709, 45101–106, 46301](#).

The FAA is publishing this Privacy Impact Assessment (PIA) for SPAS in accordance with Section 208 of the E-Government Act of 2002 because the system receives and displays Personally Identifiable Information (PII) from members of the public (air operators, air agencies, air personnel, airmen, air crew, or air maintenance personnel) including name, address, airmen certification number, date of birth and other personal information as discussed in this PIA.

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

SPAS is a read-only system that provides the ability to query multiple FAA data sources at once, as well as providing analysis tools to quantify risk, create profiles, set flags to mark trends, summarize data, and compare data sets for consideration in the oversight of air operators, air agencies, air personnel, and certificated aircraft. Only six of those FAA data sources and one external data source involve the provision of PII. This PIA focuses on those six FAA data sources and one external source system which are listed below.

SPAS receives and displays PII from the following FAA systems:

1. FAA National Tracking and Reporting Subsystem (NPTRS)/National Vital Information System (NVIS)², which is part of FAA Management Information System (FAAMIS) sends data including: airman name, home phone number, airman certificate number, date of birth (DOB), home address and airman education records. Additionally, certificate holder data (name, address, and phone number) for air operators, fractional ownership programs, air agencies, designees, check airmen, and Organizational Designation Authorization is received and displayed. The purpose of the data exchange is to populate and consolidate inspection activity and observations, including the review of qualifications of certificated airmen.
2. Enterprise Information Management Platform (EIM Platform)³ sends data (curated by a Subject Matter Expert [SME]) including National Transportation Safety Board (NTSB) data about accidents and incidents within the US, its territories, and possessions and international waters. Information includes preliminary reports, factual reports, and final descriptions of an accident with its probable cause. These reports contain crew member names, aircraft owner name and address, and operator

² The Privacy Impact Assessment (PIA) for FAAMIS is published at [Federal Aviation Administration Management Information System \(FAAMIS\) | US Department of Transportation](#)

³ The PIA for EIM platform is published at [Enterprise Information Management Platform \(EIM Platform\) | US Department of Transportation](#)



name and address. The purpose of the data exchange is to populate accident and incident data for safety analysis purposes.

3. Voluntary Disclosure Reporting Program (VDRP) sends data including disclosed violation data voluntarily submitted by airlines and their employees, including operator ID, name of air carrier or repair station making the disclosure, name of FAA inspector(s) reviewing the disclosure, corrective action taken, and user ID. The purpose of the exchange is to display VDRP data to SPAS users with pre-existing VDRP access to view the data in the same location as other data about the entity, providing a more complete profile of the entity to support analysis for oversight by the FAA Aviation Safety Inspectors (ASIs). DoD flight inspectors using SPAS do not have permissions to view VDRP data.
4. Web Operations Safety System (WebOPSS)⁴ sends data including an air operator's full name, air operator's business address, certificate number, air operator points of contact (POC) full name, air operator POC's business email address, air operator POC's business address and air operator POC's phone number. The purpose of this display is to allow SPAS users to perform analysis on air operators and air agencies.
5. FAA Accident/Incident Database Systems (AIDS)⁵ sends data including full name of the airman, DOB, airman certificate number, aircraft registration number, aircraft make and model, aircraft serial number, narrative text of the reported event, which could include information on witnesses and/or passengers related to event, and date of the accident or incident. The purpose of this display is to allow SPAS users to perform analysis of civil aviation accidents and events.
6. Safety Assurance System (SAS)⁶ sends data including: the certificate holder/airman (CH/A) full name, CH/A email address, address, phone number, airman certificate number and type, aircraft registration number, aircraft make/model/serial number, aircraft manufacturer name, engine manufacturer/mode name, and aircraft owner's full name and address and passenger's name and mailing address for the purpose of analysis of certificate holder programs and safety performance.

⁴ The PIA for WebOPSS is published at [Web-based Operations Safety System \(WebOPSS\) | US Department of Transportation](#)

⁵ The PIA for AIDS is published at [Accident and Incident Data System \(AIDS\) | US Department of Transportation](#)

⁶ The PIA for SAS will be published at [FAA Privacy Impact Assessments | US Department of Transportation](#).



SPAS sends and receives information from the Air Carrier Analysis Support (ACAS). ACAS is a DoD system supporting the Commercial Airlift Division at Air Mobility Command.

1. SPAS sends names of air operators and individuals related to safety inspection activities, airman DOB, home address, home phone number, airman certificate number, education records. The purpose of this exchange is to provide information to DOD inspectors to aid in identifying safety issues for their inspections. PII is used to correctly identify and differentiate between persons who may be the subject of an investigation or performing safety actions. VDRP data is specifically excluded from this data exchange.
2. ACAS sends air carrier and inspections information, which includes name of the air operator and names of individuals involved in or the subject of safety inspection activities. The purpose of this data exchange is to include DoD data in SPAS for analysis of aircraft events and airmen.

A Memorandum of Understanding (MOU) was initially established between the DoD and DOT in November 1998, concerning commercial aviation programs and the agreement to share aviation safety related information assists both agencies in fulfilling their statutory and regulatory responsibilities regarding air carrier fitness and safety. The agreement was updated and signed March 2024.

SPAS System Access

SPAS users consist of FAA ASIs, other FAA employees and contractors, and DoD flight inspectors. All users access SPAS using their personal identity verification (PIV) card. SPAS users access SPAS daily to evaluate safety performance, monitor trends, and review current and historical data required for informed oversight decisions.

Typical Transaction

SPAS presents data to users to analyze events affecting aviation safety and associated FAA enforcement actions and orders. The information is collected to support FAA's oversight and enforcement of compliance with safety regulations, statutes, and orders. For SPAS users to query summarized and detailed data in SPAS, the users may enter an identifier code⁷, airman certificate number, name, city and/or state. SPAS then pulls information from the

⁷An identifier code for an airman can be an airman certificate number. For an aircraft, it can be the tail number, or a unique identifier that specifies the type of aircraft; for example, Boeing 737 would appear as B-737. For an air operator or air agency certificate holder, SPAS displays the "designator code," which comes from FAA-issued certificate number. SPAS does not create or assign any of the identifier codes.



systems discussed above and displays that information to the user in a read only format. Depending on the data retrieved with a query, the result presented to the user may include DOB, education records, address, and the airman certificate number, as applicable.

The information is used to evaluate safety performance, monitor trends, and review current and historical data required for informed oversight decisions.

Records in SPAS cannot be altered. If there is an erroneous or outdated record, the change to the record in SPAS takes place in the source system. SPAS records are refreshed from the source systems an average of twice a month.

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) v3⁸, 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 Organizations⁹.

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.

SPAS does not collect information from individuals but receives information that include PII from other FAA systems and displays that information to the user in a read only format. If required, FAA provides the appropriate notice at or before the point of collection by the original source system.

Department of Transportation (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 source systems that provide information to SPAS are

⁸ <http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf>

⁹ http://csrc.nist.gov/publications/drafts/800-53-Appendix-J/IPDraft_800-53-privacy-appendix-J.pdf



subject to [DOT/FAA 847, "Aviation Records on Individuals" 89 FR 48956 \(June 10, 2024\)](#). The records in SPAS may be retrieved by airman name, certificate numbers and aircraft registration numbers. Source systems that provides information pertaining to aviation safety inspections and accident investigations are subject to [DOT/FAA 857 Accidents, Incidents and Investigations - 88 FR 73070 - October 24, 2023](#). The FAA retrieves system access records in SPAS by user 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 \(May 7, 2002\)](#).

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

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.

As noted above, SPAS does not collect information directly from individuals but receives information that include PII from other FAA and DOD systems and displays that information to the user in a read only format. Individuals have the right to request the correction, amendment, or deletion of their Privacy Act information through the source system. Under the provisions of the Privacy Act, individuals may request searches to determine if any records have been added that may pertain to them. Individuals wishing to know if their records appear in a system may inquire in person or in writing to:

Federal Aviation Administration

Privacy Office

800 Independence Ave. SW

Washington, DC 20591

Included in the request must be the following:

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



Individuals wanting to contest information about themselves that is contained in SPAS should make their requests in writing, detailing the reasons for 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 purpose of SPAS is to provide a user interface that aggregates and displays data from multiple source systems to assist SPAS users in performing aviation safety inspection activities. The PII contained in SPAS is utilized for identifying individuals related to an aircraft safety inspection or investigation.

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

1. [49 U.S.C. § 44713e](#), which requires the FAA to develop and deploy "a fully enhanced safety performance analysis system that includes automated surveillance to assist the Administrator in prioritizing and targeting surveillance and inspection activities of the Federal Aviation Administration."
2. [49 U.S.C. §§ 40101, 40113, 44701–44703, 44709, 45101–106, 46301](#), which requires the FAA to promote safe flight by establishing minimum safety inspection standards in a way that best tends to reduce or eliminate the possibility or recurrence of accidents in air transportation.

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 processing and use in SPAS to the information that is relevant and necessary to meet its authorized business purpose, which is to support FAA's oversight and enforcement of compliance with safety regulations, statutes, and orders. SPAS do not collect PII from individuals but receives the minimum amount of information from internal



and external systems to allow identification of relevant information to support oversight and enforcement.

SPAS maintains its records in accordance with:

[National Archives and Records Administration \(NARA\), General Records Schedule 5.1, approved July 2017, Common Office Records, Item 020.](#) These records are considered temporary and may be destroyed immediately after copying to a recordkeeping system or otherwise preserving. Longer retention is authorized if required.

[GRS 3.2, approved January 2023, Information Systems Security Records.](#) Item 030 allows for destruction 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 sharing of information via the SPAS system is done so in accordance with Department SORN [DOT/FAA 847, "Aviation Records on Individuals" 89 FR 48956 \(June 10, 2024\)](#). 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:

- Make airmen records available to users of FAA's Safety Performance Analysis System (SPAS), including the Department of Defense Commercial Airlift Division's Air Carrier Analysis Support System (ACAS)¹⁰ for its use in identifying safety hazards and risk areas, targeting inspection efforts for certificate holders of greatest risk, and monitoring the effectiveness of targeted oversight actions.

The sharing of information pertaining to aviation safety inspections and accident investigations in SPAS is conducted in accordance with SORN [DOT/FAA 857 Accidents, Incidents and Investigations - 88 FR 73070 - October 24, 2023](#). 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 users of FAA's Skywatch system, including the Department of Defense (DoD), the Department of Homeland Security (DHS), the Department of Justice (DOJ) and other authorized government users, information on airman, aircraft and operator records available for their use in managing, tracking, and reporting aviation-related security events.

¹⁰ ACAS is a DoD system supporting the Commercial Airlift Division at Air Mobility Command.



- To the NTSB investigators who use the data in their efforts to determine the cause of transportation accidents and incidents.

The sharing of user account information in SPAS 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 SPAS information outside DOT pursuant to 15 additional routine uses applicable to all DOT Privacy Act systems of records. These additional routine uses are published on the [U.S. Department of Transportation General Routine Uses page](#).

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).

SPAS receives information from the NPTRS/NVIS (FAAMIS), EIM Platform, VDRP, WEBOPSS, AIDS, SAS and ACAS systems and does not collect information directly from an individual. The data displayed in SPAS is assumed to be accurate. If there are any changes that need to occur to the source data, the requester must initiate those changes with the appropriate source system, where the data would be amended and subsequently transferred to SPAS.

During the file transfer from the source systems to SPAS, there is no human interface which eliminates the possibility of human error impacting the quality and integrity of the data.

Further, SPAS does not allow any user to add, delete or revise information and PII within SPAS, which helps preserve data quality and greatly reduces the opportunity for the quality



or integrity of the data to be compromised. Data protection is implemented primarily as a part of the processing and storage infrastructure. Data updates received from connecting systems are performed on a regular schedule (twice a month, on average) as agreed to by SPAS and the interconnecting systems.

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 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, dated December 2020.

SPAS 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 PIV card. All PII is encrypted in transit and at rest. SPAS is only available to authorized FAA users that access the system using their personal identity verification card. 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 SPAS, as related to the requirements of OMB Circular A-130, *Managing Information as a Strategic Resource*.

SPAS 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 SPAS administrators, privacy personnel, and security personnel have conducted a privacy/security incident response exercise to evaluate the effectiveness of this plan.

SPAS has a system security plan in place. The system was issued an Authority to Operate after completing the authorization and accreditation process that reviews security controls and procedures and that validates that SPAS 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 SPAS 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 SPAS as related to the requirements of OMB Circular A-130, Managing Information as a Strategic Resource.

Responsible Officials

Lai Lee-Birman
SPAS System Owner
Office of Solutions Delivery

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer