U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration (FAA)

Office of Aviation Safety (AVS)

Safety Assurance System (SAS)

Responsible Official

Jacob Kemnec
Email: Jacob.C.Kemnec@faa.gov
Phone Number: (206) 427-7834

Reviewing Official

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

[Publication Date]

Executive Summary

The Federal Aviation Administration (FAA) developed this Privacy Impact Assessment (PIA) for the Safety Assurance System (SAS). SAS is used to create a standardized risk-based, data-supported oversight system across Flight Standards Service (FS), Office of Hazardous Materials Safety (AXH), and other Aviation Safety (AVS) Offices. SAS is the FAA's oversight tool to perform certification, surveillance, and Continued Operational Safety (COS). SAS includes policy, processes, and associated software that FS, AXH, and other AVS Offices use to capture data when conducting oversight. SAS operates in accordance with the following authorities: 49 U.S.C. §44103, 49 U.S.C. §44701, 49 U.S.C. §44702, 49 U.S.C. §44705, 49 U.S.C. §44707, 49 CFR § 171.15 and 49 CFR § 171.16.

Under the E-Government Act of 2002, the FAA is publishing this Privacy Impact Assessment (PIA) because SAS collects Personally Identifiable Information (PII) from certificated individuals[1], Other Regulated Entities (OREs)[2], Certificate Holders/Applicants (CH/As), check airmen, and passengers.

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

[1] Certificated individuals are those individuals that have been issued an Airmen certificate.
[2] Hazardous material shippers, repair stations, freight forwarders, and ground handlers who offers hazardous materials as defined by 49 CFR 171.8.
[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).

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.

SAS is the FAA's oversight tool to perform certification, surveillance, and COS. SAS includes policy, processes, and associated software that FS, AXH, and other AVS Offices use to capture data when conducting oversight. SAS standardizes the work across FS and AXH to improves consistency and collaboration across the FAA. In addition, SAS helps FAA Aviation Safety Inspectors (ASIs) determine risk-based, data-supported oversight decisions, determine hazard identification and risk assessment strategies to formulate surveillance plans, where to focus FAA resources, and provides the standardized protocols to evaluate whether certificate holder operations are compliant with regulations. SAS accomplishes these initiatives by documenting performance of certifications, surveillance, and COS.

SAS has both external and internal users. External users are CH/As that use SAS to submit a certificate to operate, amend an existing certificate to operate or communicate with their local Flight Service District Office (FSDO). Internal users are FAA employees or contractors, such as ASIs, Principal Inspectors (PIs) and Hazardous Material Aviation Safety Inspectors (HM ASIs) that use SAS to manage the certificate to operate process and to investigate reported hazardous material incidents.

External Users

External users access SAS via https://sas.faa.gov. First-time external users are required to create an account via MyAccess by providing their name, email, and either the last four digits of their social security number or government-issued ID. See the MyAccess PIA published at MyAccess-PIA for a full discussion.

Application Submission Process

The CH/As navigate to https://sas.faa.gov to log in and manually enters the following information into SAS to submit a certificate to operate:

- Organization's name;
- Full name of main point of contact;
- Job title;
- Business address;
- Country (if foreign);
- Business telephone number; and
- Business email address.

CH/As then upload applicable supporting documentation[4] for their certificate to operate into SAS. SAS stores the supporting documentation in Document Management[5], which is the centralized repository for all of SAS electronic records. The supporting documents includes Form 8400-6, *Preapplication Statement of Intent* and either Form 8420-8, *Pilot School Certification* or Form 8310-3, *Application for Repair Station Certificate and/or Rating,* check airmen resumes and training records and management personnel's resumes. Furthermore, the CH/As can mail the supporting documentation to their local FSDO, at which point the FSDO will upload the documents into Document Management. The supporting document may include the following PII:

- CH/A's name;
- Business email address;

[4] There is a schedule of events that outline what documentation is to be provided to get certified.
[5] Document Management is an electronic repository that is recognized by National Archives and Records Administration as the official repository for records associated with Continued Operational Safety, certification, oversight management, and other SAS and Operations Safety System business processes that the automation supports.

- Business address with zip code;
- Business telephone number;
- Job title;
- Airman's name, certificate number and type;
- User ID;
- Check Airmen's name, address, email address, telephone, number and past training;
- CH/A's Chief Executive Officer's (CEO's) full name;
- CEO's email address;
- CEO's business address;
- County of CH/A's operations;
- Full name of all CH/A's contractors (repair stations only);
- Business contact information (email address, business address and telephone number) of all CH/A's contractors (repair stations only);
- FAA Designator code (an FAA-issued code for certificated entities);
- Instructor's full name and certificate number;
- Examiner's full name;
- Main operating base address;
- Satellite location address;
- Aircraft make, model, and series;
- Full name of simulator sponsor;
- Full name of person responsible for scheduling simulator;
- Simulator region ID (FAA region where simulator exists);
- Enforcement Investigative Report (EIR) number and status;
- Full name of FAA designee;
- FAA Designee identification number and type;
- FAA Designee expiration date;
- FAA Designee office code; and
- FAA Designee fax number.

Resumes may include check airmen and management personnel's full name, personal address, personal telephone number, and personal email address.
CH/As submits the certificate to operate to their local FSDO for review and approval.

Review and Approval Process
Upon receipt of the certificate to operate, the local FSDO reviews the certificate to operate request with the regulatory requirements, FAA's policy and guidance for the process, and verifies the accuracy of answers provided by the CH/A and determines if changes in the process design meet the requirements for approval and acceptance. The FSDO may manually enters comments[6] regarding their evaluation of the certificate request in an open-

[6] The comments entered into the open-text box does not include PII.

text comments box. This review process allows the CH/A and the FAA to see how the proposed changes affect the CH/A's operating profile and Comprehensive Assessment Plan (CAP) which is a quarterly plan developed by inspectors and their managers to plan and schedule oversight activities.

Once the FSDO approves the certificate to operate request, SAS updates the CH/A operating profile[7] and CAP to reflect the new information. SAS sends a notification to the CH/A to inform them of the approval of their certificate request.

CH/As can amend an existing application by submitting a change request to their FSDO for approval. Any supporting documents needed to support the change are uploaded to SAS and stored in Document Management. When the FSDO receives the change request, they would follow the same process discuss above to review, approve, and notify CH/A of the approval.

Internal Portal

SAS uses five modules to track, process and manage CH/As certification to operate process. These modules are Configuration, Planning, Resource Management, Data Collection, and Analysis Assessment Action. Additionally, there is an ORE Module and a Passenger module for work not associated with the CH/As.

Module 1 - Configuration: Configuration data consists of characteristics or attributes that describe a CH/A's scope of operations and specifications. CH/As manually enter the following information in SAS:

- Operations specifications information includes route structures, fleet size, number of aircraft in fleet, fleet composition, number of repairmen, facility locations, and number of seats in aircraft;
- Vitals include the company's CEO full name, business address, business phone number, county of operations, business fax number, and business email address; and
- Air Operator Contractors information includes all service provider company names, full names, addresses, telephone numbers, email addresses, and fax numbers.

Module 2 - Planning: The Planning module allows authorized FS and AXH personnel to establish plans for inspectors to confirm regulatory compliance of certificate holders; plan and schedule inspections of certificate holders; and assign inspectors to work activities. ASI

[7] The operating profile is a list of systems/subsystems, elements and questions that are applicable to a CH/A's scope of operations. CH/As operating profile is based on the list of the functions that a CH/A performs, as well as applicable regulatory requirements, hazard analysis, configurations information, and performance history.

use this module to create a new work activity to track accidents and incidents, track tasks progress and assign inspectors and designees.

Module 3 - Resource Management: FS and AXH Managers uses the Resource Management module to develop resource allocation based on established oversight plans. Managers assigns tasks to inspectors and designees. PII in this module may contain the name of the manager and the name of the inspector.

Module 4 - Data Collection & Activity Recording: FS and AXH use this module as a standard method for collecting results of inspections on air carriers, fractional owners (91K), air agencies, check airman, and designees. Upon completion of the inspection, the ASI navigates to http://sas-internal.faa.gov and enter the information below by selecting the appropriate check boxes, selecting from prescribed drop-down menus, attaching or manually entering the following information:

- Full name;
- Address;
- Phone number;
- Fax number;
- Email address;
- Title;
- Airmen Certificate Number (which could be the SSN), identification (ID) numbers and codes (such as designee ID, FAA ID, inspector code); and
- Aircraft registration numbers.

This area also includes investigations documentation attachments for items such as enforcements, compliance actions, complaints, incidents, and accidents. PII that may be entered includes:

- Full name;
- Home Address;
- Home Phone
- Cell number;
- Fax number; and
- Home email address.

Module 5 - Analysis Assessment Action: FS and AXH employees use this module to document compliance and for risk analysis. Through information collected through the Data Collection Module, FS and AXH employees, determine whether changes to a CH/A's configuration are necessary and/or whether additional planning, resource management, and data collection is necessary for further assessment. This area could also include

investigations documentation attachments for items such as enforcements, and compliance actions. The PII that may be entered includes the:

- Full name;
- Home Address;
- Home Phone and
- Cell number;
- Fax number; and
- Home email address.

AXH Other Regulated Entity (ORE) Module

AXH uses ORE sub-modules to track, process, and manage the ORE oversight process. These sub-modules are Configuration, Planning, Resource Management, Data Collection, and Analysis Assessment Action.

ORE Configuration: Configuration data consists of characteristics or attributes that describe an ORE organizational structure. AXH manually enters information to include the organization name and contact information to include:

- Company's CEO full name, title, business address, business phone number, business fax number, and business email address; and
- Company liaison information, full name, title, business address, business phone number, business fax number, and business email address.

ORE Planning: The Planning module allows authorized AXH personnel to establish plans for inspectors to confirm regulatory compliance of ORE entities and assign inspectors. ORE Program Managers (ORE PM) create a new work item to plan and track surveillance activities, special permit reviews, and HM incidents.

ORE Resource Management: AXH Managers use the Resource Management module to develop resource allocation based on established oversight plans. Managers assign tasks to inspectors and designees. PII in this module may contain the names of the managers and inspectors.

ORE Data Collection: AXH uses this module as a standard method for documenting and reviewing the results of inspections on ORE entities.

ORE Analysis Assessment Action:

AXH ORE PM uses this module to document compliance and conduct risk analysis. Using information collected through the Data Collection Module, AXH employees determine

whether changes to an ORE profile are necessary and whether additional planning, resource management, and data collection are required for further assessment.

Incident Reporting

Hazardous material incidents require the individual or entity that discovers the incident to report the information to the Department of Transportation (DOT) and the FAA if the mode of transportation is air by completing *DOT Form 5800.1*, *Hazardous Materials Incident Report.* AXH personnel input the following information from *Form 5800.1* into SAS:

- Name of the reporting air operator;
- Business address of the reporting air operator;
- Name and mailing address of the shipper/offeror;
- Name of the air operator's authorized representative;
- Job title of air operator's authorized representative; and
- Business address, telephone number, email address, and fax number of the air operator's authorized representative.

AXH personnel conducts the investigation against the individual or entity that offered the hazardous material shipment. If the investigation leads to enforcement actions, AXH personnel complete the investigation in the Enforcement Information System (EIS)[8].

AXH Passenger Module:

AXH is responsible for addressing suspected noncompliance with the Hazardous Materials Regulations (HMR) by passengers, including those involving carry-on baggage, checked baggage, on-the-passenger, and airport security screening checkpoints. The SAS AXH Passenger Module automates the dangerous goods safety promotion process related to suspected passenger non-compliance. Designated AXH personnel enter identified noncompliance into the SAS AXH Passenger Module.

49 CFR 175.31 requires each person, as defined by § 171.8 who discovers a hazardous materials discrepancy to notify the nearest FAA Regional or Field Security office by telephone or email (9-AWA-AXH-175-31PaxNotifications@faa.gov). Upon receipt of the notification, AXH personnel manually enter the below information into SAS. Alternatively, passenger discrepancies submissions can be made via a link on the SAS external portal. In both instances, AXH personnel collect the following data:

- Name and telephone number of the person reporting the discrepancy;
- Name of the aircraft operator;
- Specific location of the shipment concerned;

- Type of hazardous material found;
- Name of the passenger;
- Nature of the discrepancy; and
- Address of the shipper/passenger or individual responsible for the discrepancy, if known, by the air carrier.

AXH personnel evaluate all the reports for risks to determine severity and whether to proceed with an investigation that is conducted outside of SAS in EIS[8]. SAS automatically purges PII from passenger reports after 90 days.

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[9], 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[10].

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 employs multiple techniques to notify individuals of the purposes for which the FAA collects, uses, disseminates, and retains their PII within SAS. External users manually enter their contact information and uploaded supporting documentation into SAS. Notice of FAA use of the information is provided via a Privacy Act Statement at the initial point of collection.

[8] See the EIS PIA on the Department of Transportation (DOT) PIA page for a detail discussion.
[9] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf
[10] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf

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 SAS is maintained pursuant to System of Record Notice DOT/FAA 847 - *Aviation Records on Individuals* - 89 FR 48956 - June 10, 2024, DOT/FAA 856 Airmen Medical Records - 88 FR 37301 - June 07, 2023 and DOT/FAA 857 *Accidents, Incidents and Investigations* - 88 FR 73070 - October 24, 2023. System access records are maintained in accordance with DOT/ALL 13 – *Internet/Intranet Activity and Access Records* (67 FR 30757, May 7, 2002).
The publication of this PIA demonstrates DOT's commitment to provide transparency about its privacy practices to all users of SAS. Additional information about the Department's privacy program may be found at https://www.transportation.gov/privacy. Individuals may also contact the DOT Chief Privacy Officer at privacy@dot.gov.

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.

SAS is the FAA's oversight tool to perform certification, surveillance, and COS. CH/As manually enters their organization's name, POC full name, job title, business address, business telephone number, business email address and uploads supporting documentation. The CH/As can access SAS at any time to make changes to information they manually enter and upload. SAS also receives information from other FAA systems. Individual can access or amend those records at the initial point of collection. As for the passenger module, these records are not subject to the Privacy Act and SAS automatically purges PII pertaining to the passengers after 90 days.

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 this 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.

Contesting record procedures:

Individuals wanting to contest information about themselves contained in this system 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.

SAS operates in accordance with the following authorities: 49 U.S.C. §44103, 49 U.S.C. §44701, 49 U.S.C. §44702, 49 U.S.C. §44705, 49 U.S.C. §44707, 49 CFR § 171.15 and 49 CFR § 171.16. SAS is the FAA's oversight tool to perform certification, surveillance, and COS. SAS sends or receives information from the following internal systems:

Accident and Incident Data System (AIDS)[11] sends via Transmission Control Protocol (TCP) the following information related to the aviation accident or incident. The information is used to provide the number of accidents and incidents for CH/A over a 5-year period and assists in the calculation of a CH/A's risk score.

- Airman's full name
- Airman certificate number (may include airman's social security number)
- Certificate type
- Air operator's full name
- Domicile zip code
- Aircraft registration number
- Aircraft serial number
- Aircraft make and model name
- Type of injury

[11] The AIDS PIA can be accessed via https://www.transportation.gov/sites/dot.gov/files/Privacy-FAA-AIDS-PIA.

- ASI/Inspector-in-Charge (IIC)'s full name
- IIC region and office code
- Number of causalities or injuries for an accident or incident

Aircraft Registry System (ARS)[12] send the following aircraft information via a Structured Query Language (SQL) service replication in real-time. The information that is received is used to validate the aircraft information in SAS.

- Aircraft serial number (N-number)
- Aircraft owner full name
- Business address
- Aircraft make/model/serial number
- Aircraft manufacturer name
- Engine manufacturer/model name
- Certificate class and date

Aviation Safety Inspector Credential Program (110A) receives the following information that is used for reporting.

- Inspector's full name
- FAA Form 8430-13, *Request for Access to Aircraft*[13] number[14]
- DCT ID
- DCT user friendly ID
- Updated date

Comprehensive Airman Information System (CAIS), a subcomponent of ARS sends via a SQL server replication the following information daily. The information is used for oversight and validating airmen's information within SAS.

- Airman's full name
- Airman certificate number
- Certificate type

Designee Management System (DMS)[15] sends the following read-only designee data nightly via SQL Server replication. The information is used to provide workload and resourcing information on the Office Worklist so manager can view what work designees are conducting and adjust the workload of the designees as appropriate.

- Designee's full name
- Designee number and type
- Designee expiration date
- Aircraft make and model name (associated with designee oversight activity)

[12] The ARS is a PIA can be accessed via https://www.transportation.gov/sites/dot.gov/files/Privacy-FAA-ARMS-PIA.
[13] This form is restricted to internal-use only by FAA employees and is not accessible to the public.
[14] This is an 8-digit number on paper form
[15] The DMS PIA can be accessed via https://www.transportation.gov/sites/dot.gov/files/Privacy-FAA-DMS-PIA.

- Designee office code
- Designee oversight activity type name and tracking number

Enforcement Information System (EIS)[16] sends enforcement investigative report (EIR) that include the EIR number, designator code and status nightly via SQL remote-stored procedure. The information is used to supply SAS with any valid open EIR numbers relevant to a certificate in its system.

FAA Management Information System (FAAMIS)[17] sends the national airmen reference, aircraft data and simulator data nightly via SQL service broker. The purpose of the exchange is activity tracking. FAAMIS receives the following information that FAAMIS provides to other downstream system.

- Inspector's full name
- Record ID
- Activity number
- Designator code
- Aircraft make/model/series
- Airman certificate number
- Airman's full name
- Examiner's full name
- Instructor's full name
- Instructor certificate number
- Aircraft serial number
- Aircraft manufacturer name

Integrated Airmen Certification and Rating Application (IACRA)[18] receives the following information that is used to accurately plan surveillance, investigation, and certification work activities.

- Doing Business As (DBA) full name
- Inspector code
- Office code
- Airman certificate number
- CH/A full name
- Examiner name
- Instructor's full name
- Instructor certification number

[16] The EIS PIA can be accessed via https://www.transportation.gov/sites/dot.gov/files/Privacy-FAA-EIS-PIA.
[17] The FAAMIS PIA can be accessed via https://www.transportation.gov/sites/dot.gov/files/Privacy-FAA-FAAMIS-PIA.
[18] The IACRA PIA can be accessed via https://www.transportation.gov/sites/dot.gov/files/Privacy-FAA-Airman Certification System-PIA.

Simulator Inventory and Evaluation Scheduling System (SIESS) send the following information via SQL server replication on a weekly basis. The information is used to assist inspectors with the assessment of CH/A's aircraft.

- Simulator ID
- Simulator manufacture ID
- Aircraft make/model/series
- Simulator sponsor's full name
- Scheduling simulator's full name
- Simulator region ID (FAA region where simulator exists)
- Simulator designator code

Safety Performance Analysis System (SPAS)[19] receives the listed data elements below through SQL server replication in real time that is used to count the number of fatal and non-fatal accidents for CH/As over a period of 5 years and calculate a score for three risk factors, comprising the Certificate Holder Index.

- CH/A full name
- CH/A email address
- Company name
- Title
- Employee position
- Address
- Telephone number
- Airman certificate number and type
- Aircraft registration number
- Aircraft make/model/serial number
- Aircraft manufacturer name
- Engine manufacturer/mode name
- Aircraft Owner's full name
- Aircraft Owner's address

Web-Based Operations Safety System (WebOPSS)[20] sends via SQL server replications the following information that enable SAS to produce a certificate holder operating profile for each certificate holder.

- CH/A operator information
- Areas of operation
- Type of operation (passenger and/or cargo)
- Airport ID
- Airport location
- Deviations and exemptions

[19] The SPAS PIA is available at https://www.transportation.gov/individuals/privacy/privacy-impact-assessments.
[20] The WebOPSS PIA is available at https://www.transportation.gov/resources/individuals/privacy/web-based-operations-safety-system-webopss.

- Aircraft listings
- Types and numbers of aircraft
- Inspector ID
- Designator code
- Aircraft serial number
- Certificate ID
- Certificate holder name
- Aircraft registration number

FAA Directory Services (FAA DS) via TCP or UDP sends the email address to authenticate all FAA users into the system.

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 SAS to the information that is relevant and necessary to meet its authorized business purpose.

The FAA retains records and disposes of them in accordance with the National Archives and Records Administration (NARA) schedule DAA-0237-2022-0012, *Safety Assurance System.* The classes of data and their retention schedules proposed for SAS are outlined below:

- Records associated with the initial certification process of an applicant applying for an operator or air agency are destroyed after 10 years or when no longer needed for reference, whichever is sooner.
- Records concerning risk assessment information specific to certificate holders are destroyed after 10 years or when no longer needed for reference, whichever is sooner.
- Records associated with the quarterly or fiscal year surveillance plan are destroyed after 10 years or when no longer needed for reference, whichever is sooner.
- Records associated with the surveillance outcomes of certificate holders and airmen are destroyed after 10 years or when no longer needed for reference, whichever is sooner.

- Records associated with job functions accomplished by FS related to accidents, incidents, occurrences, compliance actions and other types of investigations are destroyed after 3 years or when no longer needed for reference, whichever is sooner.

- Records associated with the analysis, assessment and action taken as a result of the data collection tool responses are destroyed after 5 years or when no longer needed for reference, whichever is sooner.
- Records associated with On the Job (OJT) Training for Flight Standards employees is captured using an Activity Recording record are destroyed after 10 years or when employee has departed the FAA, whichever is sooner.
- Records created as part of the user identification and authorization process to gain access to the SAS are destroyed 10 years after employee, external user, or certificate holder has departed the agency.
- Records associated with general statistical data related to hazardous materials incorrectly transported in passenger baggage are destroyed 10 years after violation is final, passenger PII is expunged after evaluated, or when letter processed.
- Records and information shared by the external user and the Flight Standards employees to include records associated with certification process the pre-application information, baseline operating profile, schedule of events, data collection tools and any other certification documentation located in the document manager are destroyed 10 years after employee has separated the agency.
- Records associated with a certificate holder's or applicant's configuration changes to an operating profile are destroyed after 10 years or when no longer needed for reference, whichever is sooner.
- The Code of Federal Regulations (49 CFR) part 100-185 and (14 CFR) are referred to hazardous materials regulations and oversight of repair stations are destroyed after 10 years or when no longer needed for reference, whichever is sooner.

As for the passenger module, SAS automatically purges PII pertaining to the passengers after 90 days. System access records are maintained in accordance with NARA GRS 3.2, *Information Systems Security Records*, approved January 2023 and are destroyed when business uses 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 SAS information outside of DOT in accordance with 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 AIDS may be disclosed outside DOT as

a routine use pursuant to 5 U.S.C. § 552a(b)(3) to: :

- To disclose information to the National Transportation Safety Board (NTSB) in connection with its investigative responsibilities.
- To make airman, aircraft, and operator record elements available 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, for their use in managing, tracking and reporting aviation-related security events.

The FAA maintains SAS information in accordance with Department published System of Records *DOT/FAA 856, "Airmen Medical Records", June 7, 2023, 88 FR 37301*. 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 of DOT as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

- To the NTSB, entire records related to the medical suitability of specific airmen for purposes of aircraft investigation responsibilities and regulatory enforcement activities as it relates to medical certification.
- To the general public, upon request, records such as information relating to an individual's physical status or condition used to determine statistically the validity of FAA medical standards; and information relating to an individual's eligibility for medical certification, requests for exemptions from medical requirements, and requests for review of certificate denials.
- To other federal agencies, personally identifiable information about airmen for the purpose of verifying the accuracy and completeness of medical information provided to FAA in connection with applications for airmen medical certification.
- To Federal, State, local and Tribal law enforcement agencies, information about airmen when engaged in an official investigation in which an airman is involved;
- To third parties, including employers and prospective employers of such individuals, records of an individual's positive drug test result, alcohol test result of 0.04 or greater breath alcohol concentration, or refusal to submit to testing required under a DOT-required testing program. Such records will also contain the names and titles of individuals who, in their commercial capacity, administer the drug and alcohol testing programs of aviation entities; and
- To Federal, State, local, and Tribal law enforcement, national security or homeland security agencies, information about airmen whenever such agencies are engaged in the performance of threat assessments affecting the safety of transportation or national security.

The FAA maintains SAS records in accordance with Department published System of Records Notice 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. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside of 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 DoD, DHS, 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.
- To the NTSB investigators and NTSB medical officers who use the data in their efforts to determine the cause of transportation accidents and incidents.
- To Federal, State, local and Tribal law enforcement and security agencies, information about airmen, when engaged in an official investigation or security threat assessment in which airmen are involved, or which affect the safety of transportation or national security.
- To Federal, State, local, Tribal, and foreign government agencies who use toxicology services provided by the FAA, information pertaining to the toxicology study requested by the agency.

The sharing of user account information in SAS is conducted in accordance with Department *SORN DOT/ALL 13- Internet/Intranet Activity and Access Records, 67 FR 30757 (May 7, 2002),* and consistent with the General Routine Uses identified above. 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 this application may be disclosed outside DOT as a routine use pursuant to 5 U.S.C. § 552(a) (b) (3) as provided in the SORN that applies to those records.

- 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 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, 77 FR 42796, July 20, 2012, and 84 FR 55222, October 15, 2019, under ''Prefatory Statement of General Routine Uses'' (http://www.transportation.gov/privacy/privacyactnotices).

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).

SAS collects, uses, and retains data that is relevant and necessary for the purpose for which it is collected. SAS generates audit logs that track system login activity, changes to user profiles, and changes in user roles and functions. Audit logs contain the User IDs of CH/As or the email addressed of FAA users, depending on the type of user captured in the logs. SAS performs extensive edit checks on all data that is entered into the system.

The CH/A are responsible for ensuring the accuracy of information they the enter into the system. CH/As can amend an existing application by submitting a change request to their FSDO for approval. Any supporting documents needed to support the change can also be uploaded to SAS. As for the passenger module, SAS automatically purges PII pertaining to the passengers after 90 days. Lastly information received from other systems are routinely updated.

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.

SAS 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 SAS, as related to the requirements of OMB Circular A-130, Managing Information as a Strategic Resource.

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

SAS has a system security plan in place. The system was issued an Authority to Operate on May 28, 2024, after completing the authorization and accreditation process that reviews security controls and procedures and that validates that SAS 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.

DOT implements 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.

In addition to these practices, the FAA consistently implements additional policies and procedures especially as they relate to the access, protection, retention, and destruction of PII. Federal employees/contractors who work with SAS 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 and in FAA Order 1370.121B.

The FAA also conducts periodic privacy compliance reviews of SAS as related to the requirements of OMB Circular A-130, "*Managing Information as a Strategic Resource*."

Responsible Official

Jacob Kemnec
System Owner
Operations Management Portfolio Branch, AEM-110

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN MARIE GORMAN Digitally signed by KARYN MARIE GORMAN Date: 2025.01.24 15:05:30 -05'00'