# U.S. Department of Transportation

# Privacy Impact Assessment

## Federal Aviation Administration (FAA) / Office of Aviation Safety (AVS)

## Safety Assurance System (SAS)

### Responsible Official

<<NAME>>

<<TITLE>>

<<CONTACT PHONE #>>

<<CONTACT EMAIL>>

### Reviewing Official

Claire W. Barrett

Chief Privacy & Information Asset Officer

Office of the Chief Information Officer

privacy@dot.gov

**October 2018**

## Executive Summary

The Safety Assurance System (SAS) provides the FAA Flight Standards Service (AFS) with an integrated system safety approach for the certification and oversight of aviation certificate holders operating under Federal Aviation Regulation (FAR) Title 14, Code of Federal Regulations (CFR) Part 119, 121, 135 and 145. The current phase of development will include organizations that perform air operations under 14 CFR 121, 135, and 145, known as air carriers, commuter air carriers, and repair stations, respectively. The certification and oversight of these entities is mandated under 49 USC 44707, 49 USC 44705, 14 CFR 145.5, and 14 CFR 119.59. In order to effectively fulfill these obligations, the SAS must collect personally identifiable information about airmen, aircraft owners, air carriers, commuter air carriers, repair stations, and applicants for those certificates, as well as FAA employees and contractors. This Privacy Impact Assessment (PIA) describes the FAA's collection and use of this PII and the steps that have been taken to mitigate the risks associated with that collection and use.

## 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:*

- *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.*

[1]Office of Management and Budget's (OMB) definition of the PIA taken from guidance on implementing the privacy provisions of the E-Government Act of 2002 (see OMB memo of M-03-22 dated September 26, 2003).

*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 Administration (FAA) is developing the initial Privacy Threshold Analysis (PTA) for the Safety Assurance System (SAS). The SAS replaced the Air Transportation Oversight Safety System (ATOS).[4] It is used by the Office of Aviation Safety (AVS) to support the System Approach for Safety Oversight (SASO) program office's safety and risk management operations. The SAS supports the FAA by monitoring and managing aviation certificate holders as well as applicants for aviation certificates (CH/As). CH/As include airmen, air carriers, commuter airlines, repair stations and other relevant business entities, which are considered members of the public. SAS automates two broad processes for CH/As: Initial Certification and Continued Operational Safety (COS). SAS is used by all FAA local Flight Standards District Offices (FSDO)[5] and Certificate Management Offices (CMO) responsible for monitoring and managing CH/As. The SAS is hosted at the FAA Enterprise Data Center at the Mike Monroney Aeronautical Center at 6500 South Macarthur Boulevard Oklahoma City, Oklahoma 73169-6901.

[3] See 44 USC 3201-3521; 5 CFR Part 1320

[4] . The ATOS System Disposal Assessment (SDA) was adjudicated by the DOT Chief Privacy Officer on 11/4/16.

[5] Flight Standards District Office is a Regional FAA AVS office. There are approximately 82 such regional offices nationwide. The Flight Standards District Offices particularly concentrates on compliance with the United States Federal Aviation Regulations.

### *SAS Modules and Functions*

The SAS software modules provide for initial certification and COS of CH/As through Configuration, Planning, Resource Management, Data Collection, and Analysis Assessment Action.

- Module 1 – Configuration: This module is the first step in initial certification and provides information to FAA regarding the identity and particular characteristics of a certificate applicant. It is accessible by the SAS Internal (https://sas.avs.faa.gov) and External portals (https://sas.faa.gov) which are each described in detail below. The initial certification process through the External Portal is also described below.
- Module 2 – Planning: This module allows authorized internal FAA users to establish oversight plans for inspectors in order to perform regulatory compliance on certificate holders. Chief Inspectors (CI) plan inspections of certificate holders; assign inspectors to assess CHs; and schedule inspections using the planning module. The Planning Module is only accessible through the Internal Portal.
- Module 3 – Resource Management: This module allows CI's to develop resource allocation based on established oversight plans. If, for example, an assessment required resources beyond those available to an FSDO, a CI might assign staff from a neighboring FSDO to assist. This module is only accessible through the Internal Portal.
- Module 4 – Data Collection: This module, which is accessible through the Internal and External Portals, allows Safety Inspectors to collect regulatory compliance and safety data on current certificate holders and allows external users and current certificate holders to collect data on themselves utilizing the Self-

Assessment/Self- Audit for 14 Code of Federal Regulations (CFR) Part 145s. The Data Collection Tool (DCT) is the primary method used for this data collection. A DCT is a survey consisting of questions designed by the FAA to test a target system for safety and compliance. DCTs are performed both before and after certification and typically do not contain Personally Identifiable Information (PII), however some DCTs contain open text fields that could allow an inspector to inadvertently enter PII. In the infrequent cases where PII is inadvertently submitted, program staff redact the PII. The purpose of collecting data is to gather information that Principle Inspectors use to make informed decisions about the CH/A's operating systems (1) before approving or accepting them when required to do so by regulation, and (2) during recurring Performance Assessments (PAs). Future system enhancements will include all CFR Parts subject to oversight.

- Module 5 – Analysis Assessment Action: This module allows for the analysis and assessment of design, performance, and level of risk in CH/As. Based on the information collected through the Data Collection Module and DCTs, FAA staff determine whether changes to a CH's configuration (e.g. equipment at a repair station; number of seats on an airplane) are necessary and/or whether additional planning, resource management, and data collection is necessary for further assessment.

*External Portal*

*System Access*

The External Portal is a web-based application, https://sas.faa.gov that allows CH/As to: apply for an initial certificate application; amend an existing certificate; and interact with their local FSDO.

A typical transaction for the external portal begins when an applicant starts the Initial Certification process. To do so, the applicant must register for an SAS account on the external portal website. The applicant requests an SAS account by providing his or her first name, last name and email address. After submitting this information, a confirmation screen states that the request for a SAS User ID has been submitted. The registration information is sent securely to the FAA Point of Contact (POC) at the local FSDO via hypertext transfer protocol secure (HTTPS). CH/As then receive an automated email with a link to the webpage where they will choose a submission option (e.g. new certificate applicant; existing certificate holder) and continue the SAS External Portal registration process. This link is only valid for 24 hours. The link takes users to a Pre-Application Information Submission Page.

*System Functionality*

Once within the External Portal, the CH/A can continue with their certification request. At the Pre-Application Information Submission page, users manually provide the following information: Company Name; FSDO (which is located by using the FAA FSDO website); First Name, Middle Initial, Last Name; Title; Address, City, State, Zip Code, Country; Phone Number, and Email Address. On a subsequent screen, users select a radio button for the CFR regulation applicable to their business activity (14 CFR Part 121, 135, or 145). On this screen, users may also

add the following contact information for the principle base where their operations will be conducted (as opposed to their company/individual address which was previously provided): Address, City, State, Zip Code, Country. The next Pre-Application Information screen calls for: the proposed start- up date, a self-selected three-letter identifier, and management personnel (First Name, Middle Initial, Last Name; Title, and Phone Number). The next screen provides radio buttons for CH/As to select the proposed type of operation (e.g. Part 135 Air Operators, Air Carrier Certificate, Passengers and Cargo, Cargo Only, Scheduled or Non-Scheduled Operations, Single-Pilot Operator, Pilot-in-Command Operator). The following screen requests information regarding the applicable equipment or aircraft (e.g. make/model/series, seats, payload, and an open-text field for geographic area of intended operations.[6]

The subsequent screen allows users to upload the FAA Form 8400-6 Pre-Application Statement of Intent (PASI)[7] form (described below) and any additional forms required for certification and compliance. A user enters his or her name, title, and date of submission on this screen as well as additional comments which may be entered in an open text field. After the Pre-Application Information has been submitted, the users will receive an automated email confirming receipt of the information.

[6] The Pre Application Submission Pages contain no PAS. The Program is currently updating the submission pages to include a PAS.
[7] FAA 8400-6, OMB 2120-0593, Expiration 4/30/2018.

Finally, the external users sets up his or her user account and receives an SAS User ID. New external users receive automated emails from the FAA Provisioning Portal containing: a link to log in to the Provisioning Portal; a User ID; and a temporary log in password. Users then log in to the Provisioning Portal with a User ID and password; complete security questions; and, replace the temporary password with a permanent password. Users then receive an account registration confirmation message. New External Portal users are added to the FAA EXC Active Directory Domain and authenticate via User ID and password.

If they have not already done so via the manual upload process, new SAS users then complete the PASI form electronically through the SAS external portal. PASI forms may also be found online, printed, and submitted in hard copy to the local FSDO POC. The local FSDO uses the FAA Form 8400-6 to assess the size and scope of the proposed operation, and to contact the applicant. The FAA Form 8400-6 collects the following: name and the mailing address of the company/organization; address of principal base where operations will be conducted; doing business as (DBA) name; a listing of management personal (first, middle, last name; title; telephone number; and email address); any additional information that provides a better understanding of the proposed operation or business; signature, name and title of the individual providing signature; and the name of the FDSO employee who received the application. SAS users provide this information on the site itself as well as a physical form for signature.

After users have been approved for an SAS account they have full user access to the External Portal. Users then sign in to the External Portal using their SAS ID. They are then taken to the External Portal homes screen which contains a menu with the following options: Pre-application Information (discussed above); Certification Request; Configuration (which contains options for Configuration Data, Operating Profile and Repair Station Form 8310-3); Schedule of Events; Data Collection Tools; and Document Management.

- Certification Request

The Certification Request tab allows applicants to review their Applicant Information and Certification Information which they previously submitted during the pre- application phase. Applicants may also review the status of their application. It contains the following information: Designator Code[8]; Applicant Name; SAS ID; FSDO; FAA Precertification Number[9]; Proposed Type of Operation; Date of Proposed Start-up; Certification Status; Last Updated by (SAS System or User); Date and Time of Last Update; Applicant POC's Name, Email Address, Phone Number, Address, City, State, and Country.

[8] The 'Designator Code' is the first 4 characters in a user's operator certificate number issued by the FAA.

[9] The 'Precertification Number' is the temporary designation of an applicant who has stated intent to apply for an FAA certificate.

- Configuration
  - Configuration Data

    Each certificate has a configuration which describes the proposed operations and/or specifications of the certificate holder. CH's can change their configuration in the SAS external portal and submit the proposed changes to their FSDO for approval. This process is known as a Change Request.

    Configuration includes basic information for the following categories:
    - Operations specifications (e.g. number of company's Boeing 737s, number of seats on a company's particular airplane, etc.): documents how certificate holder operations are conducted. May include items, such as fleet composition, route structure, and operations specifications
      - If applicable, may also include repair station proposed ratings and capabilities.
    - Vitals: information about the company's base of operations and senior management, its route structure, fleet type, fleet size, domestic versus international operations, etc.
    - Contractors: contact information and background information for service providers that the company contracts with.

  - Operating Profile

    The Operating Profile, also known as the Certificate Holder's Operating Profile (CHOP), is a tailored list of systems/subsystems, elements, and questions that are applicable to a certificate holder's or applicant's scope of operation. SAS users create the Operating Profile (OP) in the external portal,

based on the list of the functions that a CH/A performs, as well as applicable regulatory requirements, hazards analysis, configuration information, and performance history. Based on the OP, the FAA can then plan and provide resource assessments tailored to the CH/A. The OP contains information about the applicant, such as personnel policies, procedures manuals, quality control, training and technical data, its record system, housing and facilities, tools and equipment, and parts and materials. This information is used to help determine safety risks. The OP also contains the list of assessments the FAA conducts as a part of the oversight of the CH/A.

- Repair Station Form 8310-3

  Repair Station Form 8310-3 is the application for an aviation repair station to become an authorized Part 145 Repair Station. It allows the FAA to evaluate the complexity of the proposed operation; establish a certification team based on the complexity of the certification; and, helps ensure that programs, systems, and intended methods of compliance are thoroughly reviewed, evaluated, and tested. The 8310-3 form includes name, title, and authorization signature, which certifies the individual is authorized by the repair station to make the application, as well as the FAA Safety Inspector's name, title and signature. The owner of the repair station applying for a certificate (or an individual authorized by the owner) fills out the form using the SAS External Portal or through a hard copy submission. The FSDO uses the information provided through Form 8310-3 during the repair station certification process.

- Data Collection Tools (DCTs)

  CH/As use the SAS External Portal to perform DCTs by selecting the Data Collection Tools option in the SAS home screen menu. The DCT screen provides the following option tabs: Select DCT; Prepare DCT; Enter Common Data Fields; Perform DCT; Check DCT; and Submit DCT. The Select DCT screen displays all of the DCTs that are available. The Prepare DCT tab contains information on the DCT a user has chosen to perform such as relevant regulations, policy and guidance. The Enter Common Data Fields tab contains fields for: start and end date of the DCT; an open text field for the location of the nearest airfield; a checkbox indicating "If work is offsite of the airfield, include one of the following"; radio buttons to select "address" or "longitude/latitude". Depending on the radio button selected, a user may enter information into open text fields to indicate an address (address, city, state, zip code, country) or longitude and latitude. The Perform DCT tab contains two tabs. The first tab is a list of questions from the DCT the user has chosen to perform. The second tab identifies additional information for the particular question to be answered (e.g. radio buttons to answer specifics about the question; attach supporting documents; an open text field for additional comments). The second tab will vary depending on the question and DCT selected. The Check DCT tab is used to ensure that all required information has been provided by identifying unfinished questions and questions that require additional information. It displays the number of questions completed and icons on specific questions indicating that a question has been left blank or requires additional information. A DCT

with missing or incomplete information will not appear on the final, Submit DCT tab – only a DCT that includes all required information will appear in the tab. Once all information has been entered, the DCT may be submitted using the Submit tab.

- The Schedule of event tab provides a checklist of events; drop down menus indicating the status of the event; and fields to select proposed, current, accepted baseline (i.e. accepted date), and completion dates using electronic calendars. Each event also contains an open text field for user comments.
- The Document Management button allows users to submit supporting documentation to FAA.[10] Document Management contains folders for: Formal Application, Other Certification, Configuration Changes, and Data Collection. The Formal Application folder allows CH/As to upload documents for the formal application. Users cannot submit required documents for review until all required documents have been uploaded. The Other Certification folder allows users to upload supporting documents that they believe are applicable to their application but are not listed in the Formal Application folder. The Configuration and Data Collection folders are automatically updated when users upload documents in the SAS External Portal Configuration and Data Collection pages. When uploading documents, users are provided open text fields to describe the version of the document being entered as well as additional comments.

*Internal Portal*

The internal portal is a web-based application that helps aviation Safety Inspectors perform safety oversight by: providing tools for planning and scheduling, helping to identify hazards within an environment, and helping to eliminate or control risk. All modules in the internal portal are used for both initial certification and COS. Safety Inspectors perform Design Assessments[11] (DAs) and Performance Assessments (PAs) based on system safety principles and enter all information collected via the DCT into SAS. The Internal Portal is only accessible on the FAA internal network to authorized FAA employees and contractors. An FAA AVS Manager must approve the FAA user's access to the system. Internal Portal users are authenticated by PIV identification. Authorized FAA Federal and Contract workforce employees access the SAS internal portal system at sas.avs.faa.gov.

The internal portal web site contains five interactive panes: a main Home/Links pane; a Notifications pane; a Messages pane; a Broadcasts pane and an Individual Work Plan (IWP) plane. The How/Links pane contains web links for the Safety Performance and Analysis System (SPAS); the Flight Standards Information Management System (FSIMS); WebOPPS; the SAS Resource Guide; the SAS Assistance Feedback or Enhancement (SAFE); News & Documentation; Release Notes; Historical Broadcast Messages; How to Use DCTs; and the Geographic Airport Data Display (GeoADD).

- Home/Links

  In addition to the Useful Links detailed above, the Home/Links pane contains a fly out window that contains links Inspectors use at each phase of the CH/A process. The menu has links for: Individual Work Plans; Certification Projects; Configuration (Module 1); Planning (Module 2); Resource Management (Module 3); Data Collection (Module 4); Reports (detailed in Appendix A); and Create DCTs.

[10] The supporting documents should not contain PII information, but there's always a possibility that an inspector could inadvertently upload a document that contains PII data. Again, in the infrequent cases where PII is inadvertently submitted, program staff redact the PII.

[11] An assessment is the scheduled and executed work package for assessing a single system, subsystem, or element's design or performance with regard to safety. Evaluation allows for compliance with FAA regulations and safety standards.

- Notifications Pane

  The Notifications pane allows applicants and certificate holders to communicate with Inspectors using text messages. Notifications may include limited PII included at the sender's discretion.

- Messages Pane

  Messages can be used to announce action items or to share supporting certification documents. Messages include a free-form text field in which additional information could be entered.

- Broadcast Pane

  The broadcast pane is used to convey official messages to Internal Portal users.

- IWP Pane

  The IWP pane links to an inspectors' IWPs. It provides a drop down menu which allows users to select an IWP and smaller panes detailing action items, DCTs, configuration management, and the status of each.

A typical transaction for the Internal Portal begins when a certificate holder submits a change request of configuration data through the External Portal. The Certification Project Team, including the Principal Inspector (PI), reviews the submission with the requested changes; reviews the regulatory requirements, FAA's policy and guidance for the process; verifies the questions were answered correctly; and determines if the changes in the process design meet the requirements for approval and acceptance. This review process allows the certificate holder and FAA to see how the proposed changes will impact the certificate holder's operating profile and Comprehensive Assessment Plan (CAP).[12] Once a change is approved, the certificate holder's operating profile and CAP are regenerated to reflect the new information.

*SAS Data Exchanges*

The SAS exchanges data with the following DOT/FAA internal systems (see Section 2.10 below for details):

Federal Digital System (FDsys)[13],, FAA Directory Services[14], FAA.gov, a component of the FAA Directory Services system (FAA DS)[15],SIESS[16], Web Operations Safety System (WebOPSS)[17], Comprehensive Airmen Information System (CAIS) - a component of the Civil Aviation Registry Applications (AVS Registry)[18], Aircraft Registration System (ARS) - a component of the AVS Registry[19], Enforcement Information System (EIS)[20], Flight Standards Information Management System (FSIMS)21, Safety Performance Analysis System (SPAS)22, and Enhanced Flight Standards Automation System (eFSAS)23.

[12] The CAP is a quarterly plan developed by inspectors and their managers to plan and schedule oversight activities.
[13] FDsys is a system offered by the U.S. Government Printing Office (GPO). PTA information is not available.
[14] The FAA Directory Services PTA is currently under development.
[15] The FAA DS PTA update is currently under development.
[16] The AIT Networks PTA was adjudicated by the DOT Chief Privacy Officer on 12/29/2015.
[17] The WebOPSS PTA update is currently under development.
[18] The AVS Registry PTA update is currently under review with the DOT Chief Privacy Officer.
[19] See footnote 11.
[20] The EIS PTA was adjudicated by the DOT Chief Privacy Officer on 2/6/2017.

**Members of the Public**

Airmen: Information about airmen will be collected as part of the FAA's oversight of air carriers, commuter air carriers, and repair stations. The information will be collected during en route inspections or received from the AVS Infrastructure.

- Airman Name,
- Airman Certificate number,[2]
- Certificate type (categorization of the type of Airman Certificate),
- FAA Tracking Number (FTN),
- Certificate Holder (employer, aka air carrier, commuter air carrier, or repair station), and
- Aircraft registration data.

Aircraft owners and co-owners: Information about aircraft owners and co-owners will be collected to support the FAA's oversight of air carriers, commuter air carriers, and repair stations. It will be collected in the course of oversight activities or received from the AVS Infrastructure.

- Name,
- Address, and

[2] The information within the system includes Airmen Certificate Numbers, which could be SSNs. For their convenience, some airmen have kept their Social Security Number (SSN) as their certificate number. The Civil Aviation Registry discontinued the practice of using the SSN as a certificate number for original or new certificates in June of 2002. The Civil Aviation Registry web site provides instructions for requesting a new certificate that does not include the SSN. The airman can complete the request online or mail a completed AC Form 8060-67 (10/09), Request for Change of Certificate Number to the Airmen Certification Branch, AFS-760.

- Aircraft registration data.

Air Carriers, Commuter Air Carriers, and Repair Stations and Applicants for those Certificates:[3] These entities will provide their information primarily via the Configuration Module, but some information will also be provided when by their employees when they apply for access to the External Portal. In addition, some information will be received from the Web-based Operations Safety System (WebOPSS) and the Enforcement Information System (EIS):

- Name,
- Business phone number,[4]
- Business address,
- Aircraft and simulator information
- Location,
- Areas and type of operation,
- Deviations and exemptions,
- Enforcement information,
- Certificate number, Certificate date, and Certificate status,
- "Doing Business As" name, and
- Certificate Holding District Office (CHDO).

Employees of Air Carriers, Commuter Air Carriers, Repair Stations, and Applicants for those Certificates: SAS external users will be employees of the air carriers, commuter air carriers, and repair stations or applicants for those certificates that are tracked in SAS. Representatives of these entities will manage their configuration information. Representatives will be able to apply for certificates issued by the FAA and to request changes to existing approved configurations on behalf of their employer. Representatives will submit their information when applying for access to the SAS external portal. Representatives will also submit information about their employer's key personnel (such as the CEO and other managers) into the Configuration Module. SAS will also receive information about air carrier, commuter air carrier, and repair station employees from

- WebOPSS:

- Employee name,

[3] Air carriers and repair station, or applicants for those certificates, may be sole proprietors. While the information submitted by these entities may also constitute personal information, this information is submitted as business information and is not statutorily protected by the Privacy Act of 1974. However, the Department of Transportation recognizes that unauthorized access to and/or use of this information could have serious repercussions for individuals and protects this information accordingly.

[4] Business information may be personal information presented as business information.

- Employee title,
- Employee telephone number, and
- Employee business email address.

**FAA Employees**

The FAA employees who use, or will use, SAS are part of AFS and include Principal Inspectors, Aviation Safety Inspectors (ASIs), Aviation Safety Assistants, Aviation Safety Technicians, Operations Research Analysts (ORA), managers, the SAS Program Office, and Headquarters and Regional Offices.

Managers will be responsible for performing oversight of staff involved in the certification and oversight of air carriers, commuter air carriers. Principal Inspectors will decide which inspections need to be performed; Aviation Safety Inspectors and Cabin Safety Inspectors will perform the actual inspections and will be assisted by Aviation Safety Assistants and Aviation Safety Technicians. Data Evaluation Project Managers and Data Reviews will perform quality assurance by ensuring that the data collected by Principal Inspectors meets SAS data quality standards. The SAS Program Office is currently, and will continue to be, responsible for the daily operations of the SAS system, such as ensuring overall policies are implemented, deciding new requirements, solving and implementing automation problems, and other maintenance operations. Headquarters and Regional Offices provide analytical oversight of aircraft from a national level.

SAS collects the following information about FAA employees in order to provide system access and to track employee certification and oversight activities:

- Name,
- User ID,
- Email address,
- Phone number,
- Role and function within SAS,
- District office and office code,
- Manager name(s), and
- Specialty and technical expertise.

### FAA Contractors

SAS collects information about the FAA contractors who support SAS. SAS collects the following information about FAA contractors in order to provide access to the system:

- District Office,

- Name,
- User ID, and
- Email address.

## Fair Information Practice Principles (FIPPs) Analysis

*The DOT PIA template based on the fair information pratice 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 FIPPsd 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[5], 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[6].*

### 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.*

DOT has published the Privacy Act System of Records Notices (SORN) DOT/FAA 801, Aircraft Registration System, April 11, 2000 65 FR 19518 , DOT/FAA 815, Investigative Record System, April 11, 2000, 65 FR 19520, and DOT/FAA 847 Aviation Records on Individuals, November 9, 2010 75 FR 68849 that provide notice to the public of its privacy practices regarding the collection, use, sharing, safeguarding, maintenance, and disposal of information that affect individuals and/or their personally identifiable information (PII). The Systems of Records Notices can be found at www.dot.gov/privacy.

The publication of this PIA demonstrates DOT's commitment to provide appropriate transparency into the Safety Assurance System.

### Individual Participation and Redress

*DOT should provide 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*

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

*the decision making process regarding the collection and use of their PII and be provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.*

Under the provisions of the Privacy Act, individuals may request searches of SAS to determine if any records have been added that may pertain to them. This is accomplished by the following:

Notification procedure: 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 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 that is 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 S.W. Independence Ave
Washington DC, 20024

For questions relating to privacy, go to the DOT Privacy Program, www.dot.gov/privacy

## 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 its collects, uses, maintains, or disseminates PII.*

The FAA must collect the PII described in this document in order to fulfill its legal obligation for the certification and oversight of air carriers, commuter air carriers, and repair stations. In addition, the PII of FAA inspectors and personnel involved in performing or supporting certification and oversight must be collected to allow the FAA to track who performed the inspections and inspection results.

The FAA's legal authority to collect this information can be found in 49 U.S.C. § 44705, which states that: "The Administrator of the Federal Aviation Administration shall issue an air carrier operating certificate to a person desiring to operate as an air carrier when the Administrator finds, after investigation, that the person properly and adequately is equipped and able to operate safely under this part and regulations and standards"

The authority can also be found in 14 CFR 119.59, which states that:

(a) At any time or place, the Administrator may conduct an inspection or test to determine whether a certificate holder under this part is complying with title 49 of the United States Code, applicable regulations, the certificate, or the certificate holder's operations specifications.

(b) The certificate holder must

a. Make available to the Administrator at the certificate holder's principal base of operations
   i. The certificate holder's Air Carrier Certificate of the certificate holder's Operating Certificate and the certificate holder's operations specifications; and
   ii. A current listing that will include the location and persons responsible for each record, document, and report required to be kept by the certificate holder under title 49 of the United States Code applicable to the operation of the certificate holder.

b. Allow the Administrator to make and test or inspection to determine compliance respecting any matter stated in paragraph (a) of this section.

The authority to inspect repair stations can be found in 49 U.S.C. § 44707, which states that "The Administrator of the Federal Aviation Administration may examine and rate the following air agencies…repair stations and shops that repair, alter, and maintain aircraft, aircraft engines, propellers, and appliances, on the adequacy and suitability of the equipment, facilities, and materials for, and methods of, repair and overhaul, and the competency of the individuals doing the work or giving instruction in the work."

The authority can also be found in 14 CFR § 145.5, which states that "the certificate and operations specifications issued to a certificated repair station must be available on premises for inspection by the public and the FAA."

## 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. DOT should retain PII for only as long as necessary to fulfill the specified purpose(s) and in accordance with a National Archives and Records Administration (NARA)-approved record disposition schedule.*

SAS does not have a National Archives and Records Administration (NARA)-approved Records Disposition Schedule (RDS) or SF-115 Request for Disposition Authority as of the completion of this Privacy Impact Assessment (PIA). The FAA will work with the system owner and NARA to identify or develop an appropriate RDS for the system. Records in SAS will be maintained indefinitely in accordance with 36 CFR 1225.14 until a NARA-approved RDS is in place.

## 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 FAA will use the information in SAS for the purposes described in this PIA, SORNs DOT/FAA 801, Aircraft Registration System, April 11, 2000 65 FR 19518, DOT/FAA 815, Investigative Record System, April 11, 2000, 65 FR 19520, and DOT/FAA 847 Aviation Records on Individuals, and as otherwise authorized by law. AFS employees will collect, enter, and analyze air operator, air commuter, and repair station information in order to ensure they meet and continue to meet the standards for FAA certification. PII from SAS will be sent to SPAS and eFSAS to further support certification and oversight activities.

PII in SAS may be used in support of the FAA's related aviation safety activities, such as enforcement actions. For example, if an inspector identifies a Federal Aviation Regulation (FAR) in the course of their oversight, the information collected in SAS may be used to support the resulting enforcement action.

The information in SAS is not exempt under the Freedom of Information Act (FOIA); however, in the event of a FOIA request, PII will be redacted before releasing the information.

## 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).*

Air carriers, commuter air carriers, and repair stations and applicants for those certificates will provide information about themselves, if a sole proprietor, or, if not, their organization, including their employees, directly into the Configuration Module. The information they provide should be assumed to be correct and timely. They will also enter self-assessment and audits into the Data Collection Tools (DCT) Module; this information should also be assumed to be correct and timely.

Other information will be entered into the system by Aviation Safety Inspectors in the course of their certification and oversight activities. It will be the responsibility of each individual Aviation Safety Inspector to ensure the accuracy, relevance, and timeliness of the information they enter into SAS. Data Evaluation Program Management and Data Reviewers will assess the data in SAS to ensure it meets defined data quality standards. SAS will also use automated

data input validation field checks to ensure the accuracy of the data entered, such as by requiring the appropriate text length for an entry. SAS will use many drop-down lists that are prepopulated from other systems, including the Standard Reference Tables, to reduce entry error and to ensure consistency amongst systems. The data exchange with eFSAS, a system that performs a similar function for AFS, provides an additional opportunity to confirm the accuracy of SAS data.

## Security

*DOT shall implement administrative, technical, and physical measures 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.*

Safety Assurance System (SAS) 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 is approved through the Security Authorization Process under NIST. As of the date of publication of this PIA, SAS was last authorized on October 4, 2013. In order to gain access to SAS, users must first obtain an FAA ID and then must be granted authorization to use SAS by their local office. Only inspectors, management, and analysts are granted access to the system. All passwords are handled by the FAA Active Directory system and SAS uses SSL to encrypt all data traffic.

## 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's Office of the Chief Information Officer, Office of Information Systems Security, Privacy Office is responsible for governance and administration of FAA Order 1280.1B, Protecting Personally Identifiable Information (PII). FAA Order 1280.1 implements the various privacy laws based on the Privacy Act of 1974 (the Privacy Act), the E-Government Act of 2002 (Public Law 107-347), the Federal Information Security Management Act (FISMA), Department of Transportation (DOT) privacy regulations, Office of Management and Budget (OMB) mandates, and other applicable DOT and FAA Records Management procedures and guidance.

In addition to these practices, additional policies and procedures will be consistently applied, especially as they relate to protection, retention, and destruction of records. Federal and contract employees are given clear guidance in their

duties as they relate to collecting, using, processing, and securing privacy data. Guidance will be provided in the form of mandatory annual security and privacy awareness training, as well as FAA Privacy Rules of Behavior. The FAA Privacy Office will conduct periodic privacy compliance review of SAS with the requirements of the Office of Management and Budget (OMB) Circular A-130. SAS has event logs that capture changes to data in the system. These logs capture a description of the action that occurred, who completed the action, and the date and time of the action. These logs allow the FAA to audit employee use of SAS and to hold users responsible for their management of information in the system.

## Responsible Official

Kelly Batherwich
AVS Privacy Manager
Office of Aviation Safety (AVS)
888-PRIVAC1
privacy@faa.gov

## Approval and Signature

Original signed and on file with the DOT Privacy Office

Claire W. Barrett
Chief Privacy & Information Asset Officer
Office of the Chief Information Officer

# Appendix A –