Privacy Threshold Assessment (PTA)

Federal Aviation Administration (FAA)
Office of Aviation Safety (AVS)
Safety Assurance System (SAS)

CLAIRE W BARRETT

Digitally signed by CLAIRE W BARRETT
DN: c=US, o=U.S. Government, ou=OSTHQ, ou=DOT Headquarters, cn=CLAIRE W BARRETT
Date: 2018.04.16 13:06:22 -04'00'

4/16/2018

X Claire W. Barrett

Claire W. Barrett
Departmental Chief Privacy & Information Govern...
Signed by: OSTHQ

Privacy Threshold Assessment (PTA)

The Privacy Threshold Assessment (PTA) is an analytical tool used to determine the scope of privacy risk management activities that must be executed to ensure that the Department's initiatives do not create undue privacy risks for individuals.

The Privacy Threat Assessment (PTA) is a privacy risk management tool used by the Department of Transportation (DOT) Chief Privacy Officer (CPO). The PTA determines whether a Department system[1] creates privacy risk for individuals that must be further analyzed, documented, or mitigated, and determines the need for additional privacy compliance documentation. Additional documentation can include Privacy Impact Assessments (PIAs), System of Records notices (SORNs), and Privacy Act Exemption Rules (Exemption Rules).

The majority of the Department's privacy risk emanates from its direct collection, use, storage, and sharing of Personally Identifiable Information (PII),[2] and the IT systems used to support those processes. However, privacy risk can also be created in the Department's use of paper records or other technologies. The Department may also create privacy risk for individuals through its rulemakings and information collection requirements that require other entities to collect, use, store or share PII, or deploy technologies that create privacy risk for members of the public.

To ensure that the Department appropriately identifies those activities that may create privacy risk, a PTA is required for all IT systems, technologies, proposed rulemakings, and information collections at the Department. Additionally, the PTA is used to alert other information management stakeholders of potential risks, including information security, records management and information collection management programs. It is also used by the Department's Chief Information Officer (CIO) and Associate CIO for IT Policy and Governance (Associate CIO) to support efforts to ensure compliance with other information asset requirements including, but not limited to, the Federal Records Act (FRA), the Paperwork Reduction Act (PRA), the Federal Information Security Management Act (FISMA), the Federal Information Technology Acquisition Reform Act (FITARA) and applicable Office of Management and Budget (OMB) guidance.

Each Component establishes and follows its own processes for developing, reviewing, and verifying the PTA prior to its submission to the DOT CPO. At a minimum the PTA must be reviewed by the Component business owner, information system security manager, general counsel, records officers, and privacy officer. After the Component review is completed, the Component Privacy Office will forward the PTA to the DOT Privacy Office for final

[1] For the purposes of the PTA the term "system" is used throughout document but is not limited to traditional IT systems. It can and does refer to business activity and processes, IT systems, information collection, a project, program and/or technology, and proposed rulemaking as appropriate for the context of the assessment.

[2] The term "personally identifiable information" refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

adjudication. Only PTAs watermarked "adjudicated" and electronically signed by the DOT CPO are considered final. Do NOT send the PTA directly to the DOT PO; PTAs received by the DOT CPO directly from program/business owners will not be reviewed.

If you have questions or require assistance to complete the PTA please contact your Component Privacy Officer or the DOT Privacy Office at privacy@dot.gov. Explanatory guidance for completing the PTA can be found in the PTA Development Guide found on the DOT Privacy Program website, www.dot.gov/privacy.

PROGRAM MANAGEMENT

SYSTEM name: Safety Assurance System (SAS)

Cyber Security Assessment and Management (CSAM) ID: 1996

SYSTEM MANAGER CONTACT Information:

Name: John Frye

Email: john.frye@faa.gov

Phone Number: (703) 598-9186

Is this a NEW system?

☐ **Yes** (Proceed to Section 1)
☒ **No**
☒ **Renewal:**
☐ **Modification**

Is there a PREVIOUSLY ADJUDICATED PTA for this system?

☐ **Yes:**

Date:

☒ **No**

1 SUMMARY INFORMATION

1.1 System TYPE

☒ **Information Technology and/or Information System**

Unique Investment Identifier (UII): 021-189475443

Cyber Security Assessment and Management (CSAM) ID: 1996

☐ **Paper Based:**

☐ **Rulemaking**

Rulemaking Identification Number (RIN):

Rulemaking Stage:

☐ **Notice of Proposed Rulemaking (NPRM)**
☐ **Supplemental NPRM (SNPRM)**:
☐ **Final Rule**:

Federal Register (FR) Notice:

☐ **Information Collection Request** (ICR)[3]

☐ **New Collection**

☐ **Approved Collection or Collection Renewal**

☐ **OMB Control Number:**

☐ **Control Number Expiration Date:**

☐ **Other:**

1.2 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.

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

[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.

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.

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

[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.

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.
- **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

[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.

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);

[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.

Planning (Module 2); Resource Management (Module 3); Data Collection (Module 4); Reports (detailed in Appendix A); and Create DCTs.

- 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

[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.

Information Management System (FSIMS)[21], Safety Performance Analysis System (SPAS)[22], and Enhanced Flight Standards Automation System (eFSAS)[23].

2 INFORMATION MANGEMENT

2.1 SUBJECTS of Collection

Identify the subject population(s) for whom the system collects, maintains, or disseminates PII. (Check all that apply)

☒ **Members of the public:**

☒ **Citizens or Legal Permanent Residents (LPR)**

☐ **Visitors**

☒ **Members of the DOT Federal workforce**

☒ **Members of the DOT Contract workforce**

☐ **System Does Not Collect PII.** If the system does not collect PII, proceed directly to question 2.3.

2.2 What INFORMATION ABOUT INDIVIDUALS will be collected, used, retained, or generated?

Members of the Public (airmen, air carriers and commuter airlines, repair stations or other business entities):

- Name
- Email Address
- Company Name
- Title
- Employee Position
- Address
- Telephone Number
- User ID
- DCT ID
- District Office
- Regional FAA AVS office
- Region
- Signature
- Doing Business As (DBA) Name
- Longitude/Latitude of Nearest Airfield
- FAA Precertification Number

[21] The FSIMS PTA was adjudicated by the DOT Chief Privacy Officer on 10/1/2015.
[22] The SPAS PTA update is currently under development.
[23] The eFSAS PTA update is currently under review with the DOT Chief Privacy Officer.

- Airman Certificate Number and Type
- FAA Tracking Number (FTN)[24]
- Aircraft Registration Data
  - Aircraft Registration Number
  - Aircraft Make/Model/Serial Number
  - Aircraft Manufacturer
  - Engine Manufacturer/Model
  - Aircraft Owner Name and Address
- EIS ID (Enforcement Investigative Report – EIR Number)
- Certificate Information (Certificate Number, Certificate Date, Certificate Status, Certificate Designator Code)
- IP Address
- Documents Uploaded as Attachments in SAS
- Free-Form Text Fields

Members of the DOT Federal and Contract Workforce

- Name
- Telephone Number
- Email Address
- Signature
- Title
- Regional FAA AVS office
- Region
- District Office
- DCT ID
- Free-Form Text Field

2.3 Does the system RELATE to or provide information about individuals?

☒ **Yes**:

The system collects information pertaining to certificate holders, certificate applicants, and organizations involved in aviation surveillance activities (described above in the System Overview). The system also collects information pertaining to FAA employees tasked with inspection, certification, and/or management of inspection and certification (also described above in the System Overview). SAS maintains audit logs for its IIS server which contains no PII and a Database Audit Log which contains the PII saved in the SAS database (described above).

☐ **No**

[24] The FTN (FAA Tracking Number) is assigned to airmen by the FAA after they complete their registration in IACRA. IACRA processes applications for airman certification via the web. IACRA interfaces with multiple FAA national databases to validate data and verify specific fields. IACRA automatically ensures applicants meet regulatory and policy requirements through business rules and data validation. It implements the use of digital signatures throughout the certification process. IACRA automatically forwards an Airman Certificate and/or Rating Application, FAA Form 8710-10, application and test results to the Airman Registry. SAS receives this information from the Airman Registry.

If the answer to 2.1 is "*System Does Not Collect PII*" **and** the answer to 2.3 is "*No*", you may proceed to question 2.10.
If the system collects PII or relate to individual in any way, proceed to question 2.4.

2.4 Does the system use or collect SOCIAL SECURITY NUMBERS (SSNs)? (This includes truncated SSNs)

☐ **Yes:**

Authority:

Purpose:

☒ **No**: The system does not use or collect SSNs, including truncated SSNs. Proceed to 2.6.

2.5 Has an SSN REDUCTION plan been established for the system?

☐ **Yes:**

☐ **No:**

2.6 Does the system collect PSEUDO-SSNs?

☒ **Yes:**

- The system collects Airman Certificate Numbers which is some cases, may be the airman's SSN. 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.

☐ **No**: The system does not collect pseudo-SSNs, including truncated SSNs.

2.7 Will information about individuals be retrieved or accessed by a UNIQUE IDENTIFIER associated with or assigned to an individual?

☒ **Yes**

Is there an existing Privacy Act System of Records notice (SORN) for the records retrieved or accessed by a unique identifier?

☒ **Yes:**

SORN: DOT/FAA 801, *Aircraft Registration System*, April 11, 2000 65 FR 19518
SORN: DOT/FAA 847, *Aviation Records on Individuals*, November 9, 2010 75 FR 68849
SORN*:* DOT/ALL 13, *Internet/Intranet Activity and Access Records*, May 7, 2002 67 FR 30757

☐ **No:**

Explanation:

Expected Publication:

☐ **Not Applicable:** Proceed to question 2.9

2.8 Has a Privacy Act EXEMPTION RULE been published in support of any Exemptions claimed in the SORN?

☒ **Yes**

Exemption Rule:
DOT/FAA 847, *Aviation Records on Individuals*, November 9, 2010 75 FR 68849. Records in this system that relate to administrative actions and legal enforcement actions are exempted from certain access and disclosure requirements of the Privacy Act of 1974, pursuant to 5 U.S.C. 552a(k)(2).

☐ **No**

Explanation:

Expected Publication:

☐ **Not Applicable**: SORN does not claim Privacy Act exemptions.

2.9 Has a PRIVACY IMPACT ASSESSMENT (PIA) been published for this system?

☐ **Yes:**

☒ **No**:

☐ **Not Applicable:** The most recently adjudicated PTA indicated no PIA was required for this system.

2.10 Does the system EXCHANGE (receive and/or send) DATA from another INTERNAL (DOT) or EXTERNAL (non-DOT) system or business activity?

☒ **Yes:**

Internal (DOT) Interconnections:

- Federal Digital System (FDsys): FDsys is a system offered by the U.S. Government Printing Office (GPO) that provides free online access to official publications from all three branches of the Federal Government. SAS uses FDsys as the statement of record regarding Title 14 Code of Federal Regulations Parts 121, 135, and 145 covering Air Carrier Certifications, Air Operator Certifications, and Air Agency Certifications. SAS program staff pull CFR data manually on an ad-hoc basis in an XML format from the FDsys website. There is no PII obtained through this exchange and as such there is no applicable SORN. There is no Memorandum of Understanding (MOU) for this exchange since the information is publicly available and obtained manually from a public website. FAA Directory Services – FAA Directory Services is a general services system which provides an authentication source for FAA users. Non-DOT users accessing the SAS External Portal are added to the EXC domain (part of FAA Directory Services) and authenticate via unique user ID and password. Once approved by their local FSDO Non-DOT users are added to the external FAA EXC Active Directory Domain and authenticate to the system via unique user ID and password. SORN coverage is DOT/FAA 847 *Aviation Records on Individuals*, November 9, 2010 75 FR 68849.

  SIESS: SAS has a one-way incoming interconnection with SIESS via Structured Query Language (SQL) server replication. SIESS maintains information on the capabilities and sponsors of over 1,000 simulators located in the U.S. and overseas. SIESS also contains results of the regularly scheduled evaluations of these simulators by the National Simulator Team. SIESS sends the following data elements to SAS on a weekly basis: Simulator ID, as well as the type of aircraft that the training data supports and simulator location. SAS uses SIESS data to assist in assessing CH's aircraft. No PII data is processed or exchanged during this interconnection and therefore no SORN coverage or MOU are required.

  WebOPSS: SAS has a one-way interconnection with WebOPSS via SQL server replication. Data received from WebOPSS enables SAS to produce a certificate holder operating profile (CHOP) for each CH/A. SORN coverage is DOT/FAA 847 *Aviation Records on Individuals*, November 9, 2010 75 FR 68849, and DOT/FAA 801, *Aircraft Registration System*, April 11, 2000 65 FR 19518. A MOU for this sharing is required but not been completed. The SO has been advised of the requirement. A POA&M should be created the missing MOU.

  WebOPSS sends the following data elements to SAS:

  - CH/As Operator information (Operation Specifications paragraphs), Areas of Operation, type of operation (passenger and/or cargo), Airport Data (Airport ID and Location), Deviations and Exemptions and aircraft listings, types of aircraft, number of aircraft; date, status, Certificate Holding District Office, types of aircraft, and number of aircraft.
  - PII data received from WebOPSS includes: Inspector ID, Certificate ID, Certificate Holder Name, and Aircraft ID.

- **AR:** SAS has a one-way interconnection with AR via SQL server replication on a real-time basis. The AR system contains information about registered aircraft and the registered owners of those aircraft. The AR system sends the following data elements to SAS: Aircraft Registration, Aircraft Make/Model/Serial Number, Aircraft Manufacturer, Engine Manufacturer/Model, Aircraft Owner Name and Address.[25] SORN coverage is DOT/FAA 801, *Aircraft Registration System*, April 11, 2000 65 FR 19518. A MOU for this sharing is required but not been completed. The SO has been advised of the requirement. A POA&M should be created the missing MOU.
- **EIS:** SAS has a one-way incoming interconnection with EIS via SQL remote-stored procedure. EIS is the source for Enforcement Investigative Report (EIR) numbers required by SAS; it is the primary key and the associated number to an enforcement case, not to an individual. EIS provides the following data elements to SAS: EIS ID (Enforcement Investigative Report – EIR Number), Designator, and Status. SAS uses this information to assist in tracking whether CH/As have any enforcement actions against them.[26] SORN coverage is DOT/FAA 847 *Aviation Records on Individuals*, November 9, 2010 75 FR 68849. A MOU for this sharing is required but not been completed. The SO has been advised of the requirement. A POA&M should be created the missing MOU.
- **FAA.gov:** SAS has a one-way https interconnection with the FAA.gov web service. Regulations and Policy website contains advisories and guidance, forms, FAA regulations, handbooks and manuals, orders and notices, policy and guidance, reauthorizations and regulatory documents. This is public information and does not contain any PII data elements and therefore no SORN coverage is required and no MOU is required. SAS automatically pulls Advisory Circulars from this site via a public web service.[27]
- **FSIMS:** SAS has a two-way interconnection with FSIMS to exchange aviation certification and safety information, specifically regarding FAA Order 8900.1. The outgoing information from SAS to FSIMS is sent via File Transfer Protocol (FTP). The incoming information from FSIMS to SAS is database replication of FAA Order 8900.1 to inform inspection duties. SAS sends DCTs to the FSIMS Librarian via FTP to manually upload into FSIMS. No PII data is processed or exchanged during this interconnection and therefore no SORN coverage or MOU is required.[28]
- **SPAS:** The SPAS provides users the ability to search for and view information regarding aviation safety trends. SAS provides inspection data on CHs for SPAS via a one-way interconnection to SPAS through database replication. SPAS uses

[25] The AR PTA, dated September 2011, does not state that there is an interconnection between AR and the SAS. In addition, the AR System Characterization Document dated December 2017 does not indicate that there is an interconnection between AR and the SAS.
[26] The EIS PTA, adjudicated February 2017, does not state that there is an interconnection between EIS and the SAS.
[27] The FAA.gov System Characterization Document dated October 2017 does not indicate that there is an interconnection between FAA.gov and the SAS.
[28] The FSIMS PTA, adjudicated October 2015, does not state that there is an interconnection between FSIMS and the SAS.

SAS inspection data to help assess safety concerns arising from CHs. SAS exports all SAS database fields populated by SAS users into SPAS. This includes the PII data elements listed in Section 2.2. The SAS Internal Portal also contains a link to SPAS. SORN coverage is DOT/FAA 847 *Aviation Records on Individuals*, November 9, 2010 75 FR 68849, and DOT/FAA 801, *Aircraft Registration System*, April 11, 2000 65 FR 19518. A MOU for this sharing is required but not been completed. The SO has been advised of the requirement. A POA&M should be created the missing MOU.

- **eFSAS**: eFSAS provides aviation safety inspection reports and information. SAS has a two-way interconnection via a remote procedure call with eFSAS, to exchange configuration information about CHs. CFR Parts 121, 121/135, 135 and 145 configuration data is replicated to SAS. Users can update the CH configuration information in SAS with changes being sent to eFSAS via a web service. This includes the PII data elements listed in Section 2.2. eFSAS data is replicated to SAS in order to ensure that the two databases' information regarding CHs is identical.[29] SORN coverage is DOT/FAA 847 *Aviation Records on Individuals*, November 9, 2010 75 FR 68849, and DOT/FAA 801, *Aircraft Registration System*, April 11, 2000 65 FR 19518. A MOU for this sharing is required but not been completed. The SO has been advised of the requirement. A POA&M should be created the missing MOU.

☐ **No**

2.11 Does the system have a National Archives and Records Administration (NARA)-approved RECORDS DISPOSITION schedule for system records?

☐ **Yes:**

Schedule Identifier:

Schedule Summary:

☒ **In Progress:**

On November 21, 2017 the AVS Records Officer advised that Big Bucket Schedule, DAA-0237-2016-0012-0017, has been proposed to NARA but has not yet been approved.

☐ **No:**

[29] The eFSAS PTA, dated December 2009, does not state that there is an interconnection between eFSAS and the SAS. In addition, the eFSAS System Characterization Document dated May 2017 does not indicate that there is an interconnection between eFSAS and the SAS.

3 SYSTEM LIFECYCLE

The systems development life cycle (SDLC) is a process for planning, creating, testing, and deploying an information system. Privacy risk can change depending on where a system is in its lifecycle.

3.1 Was this system IN PLACE in an ELECTRONIC FORMAT prior to 2002?

The E-Government Act of 2002 (EGov) establishes criteria for the types of systems that require additional privacy considerations. It applies to systems established in 2002 or later, or existing systems that were modified after 2002.

☐ **Yes**: Provide date was the system established as an electronic system.

☒ **No:** SAS began operation in June 2014.

☐**Not Applicable**: System is not currently an electronic system. Proceed to Section 4.

3.2 Has the system been MODIFIED in any way since 2002?

☒ **Yes**: The system has been modified since 2002.

☒ **Maintenance.**

☒ **Security.**

☐ **Changes Creating Privacy Risk**:

☒ **Other**:

- The Standard Reference Table (SRT) was moved from the SAS system boundary to the AVS SOA-I system boundary in April 2016. The SRT consists of a list of airports, county codes, and state zip codes; the SRT does not include PII data.

☐ **No**: The system has not been modified in any way since 2002.

3.3 Is the system a CONTRACTOR-owned or -managed system?

☐ **Yes**: The system is owned or managed under contract.

Contract Number:

Contractor:

☒ **No**: The system is owned and managed by Federal employees.

3.4 Has a system Security Risk CATEGORIZATION been completed?

The DOT Privacy Risk Management policy requires that all PII be protected using controls consistent with Federal Information Processing Standard Publication 199 (FIPS 199) moderate confidentiality standards. The OA Privacy Officer should be engaged in the risk determination process and take data types into account.

☒ **Yes**: A risk categorization has been completed.

Based on the risk level definitions and classifications provided above, indicate the information categorization determinations for each of the following:

Confidentiality: ☐ Low ☒ Moderate ☐ High ☐ Undefined

Integrity: ☐ Low ☒ Moderate ☐ High ☐ Undefined

Availability: ☒ Low ☐ Moderate ☐ High ☐ Undefined

Based on the risk level definitions and classifications provided above, indicate the information system categorization determinations for each of the following:

Confidentiality: ☐ Low ☒ Moderate ☐ High ☐ Undefined

Integrity: ☐ Low ☒ Moderate ☐ High ☐ Undefined

Availability: ☐ Low ☐ Moderate ☒ High ☐ Undefined

☐ **No:** A risk categorization has not been completed. Provide date of anticipated completion.

3.5 Has the system been issued an AUTHORITY TO OPERATE?

☒ **Yes:**

Date of Initial Authority to Operate (ATO): 3/24/2017

Anticipated Date of Updated ATO: 3/24/2020

☐ **No:**

☐ **Not Applicable**: System is not covered by the Federal Information Security Act (FISMA).

4 COMPONENT PRIVACY OFFICER ANALYSIS

The Component Privacy Officer (PO) is responsible for ensuring that the PTA is as complete and accurate as possible before submitting to the DOT Privacy Office for review and adjudication.

COMPONENT PRIVACY OFFICER CONTACT Information

Name: Barbara Stance

Email: Barbara.stance@faa.gov

Phone Number: 202-267-1403

COMPONENT PRIVACY OFFICER Analysis

Privacy risks exist in the Safety Assurance System (SAS) because the subjects of the PII collection in the system are Members of the Public and Members for the DOT Federal and Contract workforce. Such risks are mitigated by the implementation of administrative, technical and physical security measures which include restrictions on access to information by authorized individuals, use of userID and passwords and/or PIV, reviews of security and access logs to determine anomalous activity, and regular reviews of security procedures and best practices to enhance security. FAA employees and contractors are additionally required to complete annual privacy and security training.

A risk exists because the FAA does not currently have an approved ICR that will be expiring for the current collection of the information. The program office is working with the PRA office to update and mitigate this risk. A risk also exists because the FAA may inadvertently receive PII information in supporting documents that was not requested. This risk is mitigated by program staff who redact the PII if not needed. There is a risk that the information collected could be used for unauthorized purposes that are inconsistent with the original purpose of collection. This risk is mitigated because the FAA is required to protect and use data in accordance with the policies, standards, and specified regulations. There is risk that the information being shared may not be covered by a current sharing agreement. This risk is mitigated by FAA working with system owners to ensure that a MOU or access agreement is executed if required. A risk exists relative to non-completed and adjudicated privacy plan documents; this risk is being mitigated by working with the SO's to complete the required documentation.

The records are covered under: DOT/FAA 801, Aircraft Registration System, April 11, 2000 65 FR 19518 and SORN: DOT/FAA 847, Aviation Records on Individuals, November 9, 2010 75 FR 68849. Activity and Access records are covered under DOT/ALL 13, Internet/Intranet Activity and Access Records, May 7, 2002 67 FR 30757.

Records are additionally maintained in accordance with a Big Bucket Schedule, DAA-0237-2016-0012-0017, that has been proposed to NARA but has not yet been approved.

COMPONENT PRIVACY OFFICER Analysis

5 COMPONENT REVIEW

Prior to submitting the PTA for adjudication, it is critical that the oversight offices within the Component have reviewed the PTA for completeness, comprehension and accuracy.

Component Reviewer	Name	Review Date
Business Owner	John Frye	2/6/2018
General Counsel	Michael McKinley	4/6/18
Information System Security Manager (ISSM)	None	None
Privacy Officer	Barbara Stance	*3/15/18*
Records Officer	Kelly Batherwich	2/6/18

/Table 1 - Individuals who have reviewed the PTA and attest to its completeness, comprehension and accuracy.

TO BE COMPLETED BY THE DOT PRIVACY OFFICE

Adjudication Review COMPLETED: April 16, 2018

DOT Privacy Office REVIEWER: Claire W. Barrett

DESIGNATION

☐ **This is NOT a Privacy Sensitive System – the system contains no Personally Identifiable Information.**

☒ **This IS a Privacy Sensitive System**

☐ **IT System.**
☐ **National Security System.**
☐ **Legacy System.**
☐ **HR System.**
☐ **Rule.**
☒ **Other:** Aviation Safety Non-NAS

DETERMINATION

☐ ***PTA is sufficient at this time.***

☐ ***Privacy compliance documentation determination in progress.***

PIA

☐ ***PIA is not required at this time:*** Please see adjudication statement.

☒ ***PIA is required.***

☐ ***System covered by existing PIA:*** <<*Identify PIA*>>

☒ ***New PIA is required.*** Leverages new IT to collect information about individuals

☐ ***PIA update is required.*** <<*Rationale*>>

SORN

☐ ***SORN not required at this time.*** System does not collect information in identifiable form.

☒ ***SORN is required.***

☒ ***System covered by existing SORN:*** DOT/FAA 801, *Aircraft Registration System*, April 11, 2000 65 FR 19518 and

☐ ***New SORN is required.*** <<*Rationale*>>

☒ **SORN update is required**. DOT/FAA 847, *Aviation Records on Individuals*, November 9, 2010 75 FR 68849 – Exemption information not complete, Exemption rule not published for

DOT CHIEF PRIVACY OFFICER COMMENTS

The DOT Privacy Officer (DOT PO) has determined that the Safety Assurance System (SAS)collects personally identifiable information (PII) on individuals and constitutes a privacy sensitive system. T

The System was developed after to implementation of the E-Government Act and a Privacy Impact Assessment (PIA) is required before, "developing or procuring IT systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public." See "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002" (M-03-22) Within 30 days of the PTA adjudication a PIA must be submitted for approval by the DOT CPO. If a PIA is not received by that date the DOT CPO may recommend to the Senior Agency Official for Privacy (SAOP) that the system be removed from operational status until the system has a fully approved privacy plan. The FAA is recommended to establish a Plan of Actions and Milestones (POA&M) for control AR-2/Privacy Impact and Risk Assessment.

Information in the system is retrieved by personal identifier and meets the standard for a system of records as defined by the Privacy Act. The appropriate system of record notices (SORNs) for records related **to the primary purpose of the system are** DOT/FAA 801, *Aircraft Registration System*, April 11, 2000 65 FR 19518 and DOT/FAA 847, *Aviation Records on Individuals*, November 9, 2010 75 FR 68849. Portions of the records by DOT/FAA 847 may be exempt from portions of the Privacy Act – exemptions for the system have been codified in the DOT Regulations at 49 CFR Part 10, however the DOT CPO does not have evidence of proper rulemaking in support of this activity. In addition, the DOT/FAA 847 notice does not accurately describe the Exemptions claimed for the system. Within 90 days of the PTA adjudication an updated SORN and Exemption Rule must be submitted for approval by the DOT CPO. If the SORN and accompanying Exemption Rule are not received by that date the DOT CPO may recommend to the SAOP that the system be removed from operational status until the system has a fully approved privacy plan. The SORN and the Exemption Rule should follow the requirements established in OMB A-108, Federal Agency Responsibilities for Review, Reporting, and Publication. The FAA is recommended to establish a Plan of Actions and Milestones (POA&M) for controls TR-1/Privacy Notice and TR-2/System of Records Notices and Privacy Act Statements

NOTE: The appropriate system of records notice (SORN) for records related to technical access and administration of the system is DOT/ALL 13 - Internet/Intranet Activity and Access Records - 67 FR 30757 - May 7, 2002.

The DOT Privacy Risk Management Policy requires all authorized internal sharing of PII be documented via a Memorandum of Understanding (MOU) or other approved instrument that articulates the conditions of access and use. The FAA identified multiple instances where agreement on limited use consistent with applicable SORN or other notice given to individuals has not be executed. The FAA is recommended to establish a POA&M for control UL-1/Internal Use for each of the sharing listed in the PTA.
The FAA has asserted that it intends to apply a big-bucket schedule to records maintained in the system. However, the FAA has not provided support that the schedule was coordinated with the privacy program to ensure that proposed retention of records protected under the Privacy Act is

consistent with published notices. Within 30 days of the PTA adjudication a copy of the schedule submitted to NARA for approval and an accompanying privacy analysis for the Privacy Act records covered by the proposed schedule should be provided to the DOT CPO . If the Requested information is not received by that date the DOT CPO may recommend to the SAOP that the system be removed from operational status until the system has a fully approved privacy plan. In addition, the DOT CPO may request the Senior Agency Official for Records Management (SAORM) recall the pending schedule from NARA until agreement on limited retention is reached. Additionally, the SAS replaces functionality of a previously existing system ATOS/SAS – it is unclear why the records schedule covering that system has not been directly applied to this system. The FAA is recommended to establish a POA&M for controls DM-2/Data Retention and Disposal and SI-12/Information Handling and Retention.

NOTE: In its 2014 Quality Control Review of Controls Over DOT's Protection of Privacy Information the DOT Inspector General noted that Departmental IT systems need to improve "ongoing validation of specific privacy related security controls for their systems are in effect, including those that safeguard confidentiality, provide secure remote access, encryption of back up media, follow up of unauthorized mobile devices, and proper user account and password settings in accordance with DOT policy. " FAA management is strongly encouraged to review NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) and make an active determination regarding the applicability of the specific security controls identified in section 4.3 of the same.

The FAA was notified in the ATOS/SAS system disposal assessment (SDA) ATOS/SAS and that the recipient system SAS required a full privacy risk management plan prior to operations. The FAA granted the system without conducting a preliminary privacy risk assessment in the form of the privacy threshold analysis (PTA). The FAA is required to establish a POA&M for controls CA-1/Security Assessment and Authorization Policy and Procedures and AR-1(b)/Governance and Privacy Program (Privacy Plan) until all privacy risk management issues identified in the adjudication statement are mitigated and approved for closure by the DOT CPO.

The adjudicated PTA should be uploaded into CSAM as evidence that the required privacy analysis for this system has been completed and CSAM entries modified as appropriate to reflect the disposition.

The PTA should be updated not later than the next authorization for the information collection (if applicable), new privacy risk is introduced into the system (such as those described in the note, above), or the PTA expiration (3 years from the date of adjudication), whichever is soonest, and must be approved by the DOT CPO prior to any new collection or use of the data.

Appendix A

SAS Standard Reports

SAS reports allow users to generate reports matching selected criteria. The table below provides a brief description of each standard report. Reports are protected by role-based access. In addition, the report rolls are maintained in Tableau, not SAS and the Tableau environment is only visible inside the FAA. Select a hyperlink from the menu to the left for report samples.

Configuration [Module 1]	
Contractor/Maintenance Provider List	The Contractor/Maintenance Provider List report displays the Maintenance Providers (including Essential Maintenance Providers) and Training contractors as entered by 14 CFR part 121 and 121/135 certificate holders as part of Configuration Data under the Contractors tab. The report contains the following PII: Business Name; Business Address; Region, FAA Regional Office.
Operating Profile Report	The Operating Profile report allows users to view the Operating Profile of a selected certificate holder or to search on the set of certificate holders that have the same functions. The report contains the following PII: Region, FAA Regional Office; Business Name.
Pre-application Report	This report lists the status of the PASI form and pre-application information that has been submitted to FAA (e.g. date submitted, accepted). The report contains the following PII: FAA Regional Office; Business Name, Name.
Planning [Module 2]	
CHAT Report	This report displays details of the Certificate Holder Assessment Tool (CHAT) records. The report can be used by inspectors to see the list of CHAT updates and the related Risk Indicators that have been selected by a Principal Inspector for a CH or set of CHs. The report contains the following PII: FAA Regional Office; Business Name, Principal Investigator's comments.
Resource Management [Module 3]	

Geographic Routing History Report	This report displays the routing history of Geographic resource requests (GEOs) through the lifecycle of the GEO request. The report contains the following PII: FAA Regional Office; DCT ID; Name.
Geographic Summary Report	The Geographic Summary report provides the total counts of Geographic resource requests by status type. The report contains the following PII: FAA Regional Office; Business Name.
Resource Shortfall Report	The Resource Shortfall report displays the DCTs that have been assigned with "Resource Not Available" (RNA) status. The report contains the following PII: FAA Regional Office; Business Name; Name.
Data Collection [Module 4]	
Count of DCTs by Status Report	This report provides a graphical representation, in the form of a bar graph, of the total counts of DCTs by status. It displays the DCT Status on the horizontal axis and the total counts by Specialty (AW/OP) on the vertical axis. This report contains no PII.
DCT Findings Report	The DCT Findings report is organized by DCT Title and DCT ID to display all the question responses by response type (e.g., negative, positive, N/A, and Not Observable - N/O). The report contains the following PII: FAA Regional Office; Business Name; Name; DCT ID; Additional Comments.
DCT Status Report	This report is designed to help an office track the status of DCTs for a specified quarter. It assists in tracking DCTs through all the phases of the SAS lifecycle. The report contains the following PII: Business Name; Name;; DCT ID.
8430-13 Report	The 8430-13 report provides office managers using SAS with a list of the 8430-13 numbers used by resources in their office. An 8430-13 is a number on a physical paper form that is part of a booklet. Inspectors fill the forms out when performing inspections as part of their job function. The report contains the following PII: FAA Regional Office; Business Name; Name; DCT ID.

Analysis, Assessment and Action (AAA) [Module 5]	
Action Item Tracking Tool (AITT) Report	The Action Item Tracking Tool (AITT) report provides actions listed by CH/A, Office, and Source as submitted and updated by users. The report contains the following PII: Name
Assessment Determination and Actions Report	The Assessment Determination and Actions report lists all of the assessment determinations and related actions for CH/As based on the criteria entered by the user. It displays details about the determination including the justification text and details about which actions (if any) were selected. This report contains the following PII: FAA Regional Office.
Assessment Findings Report	The Assessment Findings Report provides the question response data type (e.g., positive, negative, N/A, and N/O) by DCT within assessments. The report contains the following PII: Name.
User Administration	
Roster Report	The Roster report provides details on internal SAS users. The report contains the following PII: Name; User ID; Email Address; Telephone Number; Office; Title; Region.
Proxy Report	The Proxy report provides users with a list of the proxy assignments based on the search criteria entered. This report is useful to understand which users are assigned as a proxy on the behalf of other users. The report is a two-part report. The first set of data, for single SAS user record, displays the user(s) that are assigned as a proxy to that user and in what roles. The second set of data displays the users and their respective roles that the user is acting as a proxy for. The report contains the following PII: Name; Office; Region.
External User Roster Report	The External User Roster report provides users with a list of external users This report is useful for internal SAS users to quickly find the contact information for an external contact. The report contains the following PII: Name; Email Address; Telephone Number; Business Name; District Office.

Audit Reports	
Login History Report	The Login History report provides the Security Auditors with the login history for internal and external users presented based on the search criteria entered. The report contains the following PII: Region, Office, Name.
Unsuccessful Login Attempt Report	The Unsuccessful Login Attempt report displays the attempted logins by inactive internal SAS users and external SAS users. The data displays inactive internal SAS users that are on the FAA domain that attempt to login, active external SAS users that attempt to log in with an incorrect password, and inactive external SAS users that attempt to log in. The report displays the following PII: Region, Office, Name; User ID; IP Address.
User Account Change Report	The User Account Change report displays records of internal and external SAS user accounts have been enabled, disabled, or modified. The report displays the following PII: Region, Office, Name.