Privacy Threshold Assessment (PTA)

Federal Aviation Administration (FAA)
Office of Airports (ARP)
System of Airports Reporting (SOAR)

CLAIRE W BARRETT Digitally signed by CLAIRE W BARRETT
Date: 2020.12.14 11:22:10 -05'00'

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: System of Airports Reporting (SOAR)

Cyber Security Assessment and Management (CSAM) ID: 1356

SYSTEM MANAGER CONTACT Information:

Name: Cynthia Flores

Email: cynthia.flores@faa.gov

Phone Number: 202-267-5461

Is this a NEW system?

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

Is there a PREVIOUSLY ADJUDICATED PTA for this system?

☒ **Yes:**

Date: 09/26/2018

☐ **No**

1 SUMMARY INFORMATION

1.1 System TYPE

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

Unique Investment Identifier (UII): 021-550799054

Cyber Security Assessment and Management (CSAM) ID: 1356

☐ **Paper Based:**

☐ **Rulemaking**

Rulemaking Identification Number (RIN):

Rulemaking Stage:

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

Federal Register (FR) Notice: Click here to enter text.

☐ **Information Collection Request** (ICR)[3]
- ☐ **New Collection**
- ☐ **Approved Collection or Collection Renewal**
  - ☐ **OMB Control Number:**
  - ☐ **Control Number Expiration Date:**

☐ **Other:**

1.2 System OVERVIEW:

This is an update to the previously-adjudicated Privacy Threshold Assessment (PTA) for the System of Airports Reporting (SOAR), dated September 26, 2018. SOAR is the Federal Aviation Administration (FAA) system used to track grant applications and funding transfers between the Department of Transportation (DOT) and airports across the United States in order to administer the Airport Improvement Program (AIP)[4] and the Passenger Facility Charge (PFC)[5] program. SOAR servers are deployed at the William J. Hughes Technical Center in Atlantic City, New Jersey. This PTA provides the following updates:

(1) The Personally Identifiable Information (PII) present in SOAR is business contact information for airport sponsors and public agencies.
(2) SOAR has completed the migration of the SOAR-Demo web server and supporting database to the FAA Amazon Web Services GovCloud (FCS AWS GovCloud)[6] platform; however, only a SOAR test server is currently located in the cloud platform at this time.

The System Owner has submitted a change request for the input form to change the use of "personal" to "user" on the data entry form. While information is captured from members of the public, these individuals are sponsor, congressional and aviation industry liaisons who provide business related information on themselves and their respective organizations.

SOAR is comprised of two subsystems: SOAR External (referred to as the Airport External Portal (AEP)) and SOAR Internal.

SOAR External - AEP
SOAR External AEP is a public-facing website, hosted securely using Secured Socket Layer (SSL) encryption, and is available at https://aep.airports.faa.gov/Default.aspx. The users of this subsystem are non-FAA aviation (airports, sponsors, public agencies, and air

[3] See 44 USC 3201-3521; 5 CFR Part 1320
[4] AIP is a major grant program for the planning, construction, improvement, and repair of United States airports.
[5] The PFC program allows public agencies controlling public-owned commercial service airports to impose a fee on air travelers and to use the funds for approved projects. The PFC program is authorized by 49 U.S.C. § 40117.
[6] FCS AWS GovCloud (CSAM #2092) has an adjudicated PTA, dated 08/16/2019.

carriers) employees. These external users are members of the public, and the website contains a direct link to the FAA Privacy Policy.

To create an account, external users must complete the "New User Request Account" web form, where they manually enter their name, title, business email address, business address, city, state, zip code, country, and phone number. External users are also prompted to create security questions and answers.[7] Once the request is submitted, it is reviewed by the SOAR Program Manager. If access is approved, AEP will generate an email notification that includes a username and password which is sent to the external requestor's business email address.

The AEP website does not include a Privacy Act Statement (PAS). The Program is currently coordinating with the FAA Chief Privacy Office and Office of General Counsel to develop a PAS for inclusion on the AEP website.

Once external users have access to AEP, they can perform multiple transactions related to the airport(s) and program(s) they represent. For example, external users can manually input airport and air carrier contact information (such as full name, business street address, city, state, zip, phone, and business email address) for the purpose of generating profiles from which they can enter quarterly PFC financial data for a specified airport by entering revenue details for specified calendar years. There is no data retrieval by identifiers.

AEP provides access to pre-generated reports meant for external users as well as five (5) reports that are publicly-available (log in is not required to access the publicly available reports). These reports are related to the collection of PFC for certain time periods, including interest accrued, and revenue. These external reports do not include any PII.

SOAR Internal

SOAR Internal is accessible to internal users on the FAA intranet at https://soar.arp.faa.gov using MyAccess[8] authentication. The users of SOAR Internal are ARP federal and contract employees.

The Security Control (SC)-8 POA&M in CSAM was closed once the SSL encryption was added to this module.

SOAR Internal is comprised of the following modules:

SOAR Air Carrier Activity Information System (ACAIS): This module is the primary source for the viewing, editing, and addition of airport, carrier, enplanement, and cargo information.

[7] Security questions include: "What school did you attend for the 5th grade?" "What is your preferred musical genre?" "What was the model year of your first car?"
[8] MyAccess (CSAM #2009) has an adjudicated PTA, dated 12/20/2016, which is expired.

The main data input is via the Airport Activity Survey, Form 1800-31,[9] which can be submitted in the following ways: 1) electronically with direct input to ACAIS; 2) email; or 3) hardcopy. These submissions require the user to input the operator name and address, FAA Certificate Information Number (with Issue Date), Airport Location Identifier (i.e. CON for the Concord, New Hampshire airport), and the name, title and signature of the preparing official. For users who choose to submit via email, the air carriers manually complete the form, certify to accuracy of the data by signing it, and submit the form to the FAA group mailbox where the data is manually entered in the system. Alternatively, they may send a hard copy of the form to the contractor (Booz Allen)'s office for manual data entry into SOAR. With this data, the ACAIS can generate reports on enplanement statistics on the respective airport(s).

SOAR National Plan of Integrated Airport Systems (NPIAS): This data usage module is used to determine the amount of funds the airport is entitled to. The NPIAS module consists of statistical data entry and reporting to track the cargo and passenger landings for a given calendar year. Reports generated include statistical reports and may contain airport contact information (such as airport data, carrier data, and business contact information).

SOAR AIP (Grants): The AIP, which is established under chapter 471 of title 49, United States Code (U.S.C.), is a grant program for the construction, improvement, and preservation of airports identified in the NPIAS. The AIP module performs calculations that enable users to quickly determine grant qualifications and entitlements. It provides a series of pages through which the user creates a grant, and then tracks the grant through an iterative approval process until the grant is released. The AIP module also tracks all funding associated with a grant and its projects until the grant is closed. Within SOAR, the AIP module combines two major functional requirements: Grants Processing and Funds Management.

Grants Processing: This function tracks and reports on grants from the application, to award, and final close out. The system users enter information such as airport name/worksite, fiscal year, location, grant type, funding information (such as limitation codes, amount available, changed amount, and length of grant). The user can then enter project information about a specific grant, such as "rehabilitate taxiway". The grant is then processed through multiple reviews, and can be approved, deleted/withdrawn, modified, amended, or reported on.

The Office of Government and Industry Affairs (AGI) is the principal advisor to the Office of Airports on all matters concerning Congress, aviation industry groups, and other governmental organizations. As such,

[9] OMB Control number: 2120-0067, expiration date 02/29/2020. Note: The ICR has an approved extension until 10/31/2020. Calendar year enplanement data is due by 9/30/2020.

FAA-form-1800-31-atco-2019.pdf

AGI serves as the primary point of contact on AIP and requires ability to edit/change congressional information (i.e., U.S. Senator's name, title, party affiliation, business email address, address and phone number) to ensure it is accurate before the mandatory release of grant information to Congress. No PII is released with grants information to Congress.

Once a grant is created and approved, a Grant Offer Document and Grant Transmittal Letter are generated and contain the grant, sponsor, worksite, project, Point of Contact (POC) and funding information which are provided to the specified airport or sponsor (such as the Maryland Aviation Administration).

For long term development projects, the FAA signs a Letter of Intent (LOI) with the sponsor for the parties to promise a certain level of grant funding throughout its duration. The LOI contains sponsor, project, worksite, and future funding information and could include POC name and business address.

***Funds Management*:** The Funds Management function maintains a listing of fund grant allocations, past and present, for a wide variety of purposes in order to oversee the funds distribution, as required by statute. These users can enter budgetary information on a state by state and regional basis. Users can also review accounting transactions and funding ceilings. PII is not present in this module. This data is electronically input (via spreadsheet upload) into SOAR in the form of checkbooks obtained from the Grants Notification System (GNS), a DOT system.

Users can generate over 200 reports within the AIP module, such as the enplanement report, reconciliation report, PFC adjustment report, and de-obligations report. However, only a few of those reports could contain PII including business contact information for federal employees (such as political/congressional liaisons), as well as contact information for members of the public, such as airport liaisons.

SOAR PFC: This module tracks PFC applications, associated projects, and collected revenue. PFC applications are submitted by a Public Agency (PA)[10] and serve as initial requests to impose passenger facility charges on airline tickets and use the funds collected for eligible projects. ARP staff receives the applications via various methods (i.e. email, regular mail, in person), and manually enter application data into SOAR. The types of data entered include: sponsor type, district office, congressional district, Delphi[11] Supplier Number, business

[10] Public agency means a State or any agency of one or more States; a municipality or other political subdivision of a State; an authority created by Federal, State or local law; a tax-supported organization; an Indian tribe or pueblo that controls a commercial service airport; or for the purposes of this part, a private sponsor of an airport approved to participate in the Pilot Program on Private Ownership of Airports. 14 C.F.R. 158.3
[11] Delphi is DOT's core accounting system.

Taxpayer Identification Number (TIN), and a Dun & Bradstreet (DUNS) number. A TIN is a required field that is captured when a new sponsor (i.e. business entity) is manually entered into the system. The name and business phone number of the airport's manager is electronically imported from the National Airspace System Resources (NASR).

There is no intent to collect SSN as the TIN is taxpayer information for the respective business entities, rather than the individuals themselves.

For a list of data exchanges, please see section 2.10.

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?

Subsystem/Module	Member of the DOT Federal/Contract Workforce	Member of the Public
AEP	• First name • Middle initial • Last name • User ID • Title • Line of Business and routing symbol • Business email • Fax number	• First name • Middle initial • Last name • User ID • Title • Company name • Business email • Fax number • Country

	• Country • Business Phone • Business Address • Security questions/answers • Password	• Business phone • Mobile phone • Pager number • Car phone number • Emergency phone • Organization • Country/region • Business address • Security questions/answers • Password
SOAR Internal	• Name • User ID • For contractors, company name. • Title (Optional) • For FAA employees, Line of business and routing symbol • Fax number (optional) • Business Email • Business Phone • Business Address • Password (note: SOAR no longer collects password, but there is still old, un-usable data in this field)	• First name • Middle initial • Last name • User ID (note: only for users prior to 2001) • Title • Company Name • Business email (the user are not prohibited from using non-organization email (e.g., yahoo account) • Fax number • Country • Business Phone (SOAR does not prohibit user from entering personal phone) • Mobile phone • Pager number • Car phone number • Emergency phone • Organization • Country/region • Business Address • Password (note: this is only for users that were created prior to 2011 and is no longer valid or used) • Business TIN

User IDs are maintained in audit logs.

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

☒ **Yes**:

SOAR maintains information on users of the system for access, authentication, and contact purposes. SOAR also maintains airports and sponsor liaison and accounting information for processing and reporting purposes.

☐ **No**

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:** SOAR maintains (business) TINs for sponsor organizations/airports. In the case of sole proprietorships, TINs could be a proprietor's SSN. TIN is manually added by users for cases of a mismatch with Delphi for funding reconciliation purposes. These TINs are encrypted in the system.

☐ **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/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:

☐ **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**: A PIA is in development.

☐ **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 Data Exchanges:

- NASR: SOAR pulls from NASR, via an Oracle File View, the following fields: worksite information, runway information, the names and business phone numbers of airport managers for the purpose of maintaining accurate information

on airports and sponsors. No SORN coverage is required as this data is business contact information.

NASR and SOAR do not have a PII Data Sharing Agreement. The Program is advised to develop this agreement.

- Grants Notification System (GNS): SOAR has a non-PII data exchange with GNS, a DOT system. During grant season, every 30 minutes, GNS automatically extracts grant data from the SOAR database and populates a GNS feed table via a database link. SOAR simultaneously pulls the GNS processed grants data into its system via the same database link. SOAR and GNS have a current Interconnection Security Agreement and a Memorandum of Understanding. The purpose of this exchange is to ensure accurate grant information is accounted for within SOAR. No SORN is required.

- DTF: SOAR pulls from DTF, via an Oracle Database link, non-PII accounting data regarding grant obligation, invoice and payment data. The purpose of this exchange is to ensure accurate accounting information is maintained within SOAR. No SORN or MOU is required

- MyAccess: SOAR uses MyAccess as an authentication mechanism. MyAccess sends a user's business contact information including email, active directory name to SOAR Internal. None of the data sent from MyAccess to SOAR is stored in the database as data is removed once authentication is completed. SOAR only uses the provided email address for authentication. SORN coverage is provided via DOT/ALL 13.

  SOAR and MyAccess do not have a PII Data Sharing Agreement. The current plan is for MyAccess to draft a universal PII Data Sharing Agreement for all systems it shares data with; however, the FAA has not yet started development of this Agreement.

- Flight Standards Data: Flight Standards data is the air taxi commercial operators contact information and is published by the Office of Flight Standards Service. SOAR administrators manually download a Flight Standards data file from a publicly-available web page every year and upload the data into SOAR. The purpose of this exchange is to populate Flight Standards contact data. This exchange does not require a SORN or MOU.

- Terminal Area Forecast (TAF): A member of Airport Planning and Programming (APP-400) provides the SOAR system administrator with forecast data from the TAF publicly-available web page. This data is then manually uploaded into SOAR. The purpose of this exchange is to provide SOAR with enplanement forecast data for planning purposes. No PII is included and no SORN or MOU is required.

External Data Exchanges:

- USASpending.gov: A public, government transparency website (external to DOT) wherein SOAR users manually transfer grant data from SOAR into USASpending.gov for the purpose of populating grant information on that website.
- Bureau of Transportation Statistics (BTS): The SOAR System Administrator requests enplanement data from the BTS every year for manual upload into SOAR. The purpose of this data exchange is for SOAR to maintain accurate and complete enplanement data.
  No MOUs are required for this external, non-PII data exchange.

☐ **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** The Program currently maintains SOAR records as permanent. The SOAR Program and the Records Management Office are in discussion to regarding updating the Office of Airports retention schedules, including for SOAR. This effort has been delayed, but is ongoing.

☐ **No:**

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**:

☒ **No:**

☐**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**:

☐ **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: DTFAWA-12-D-00060

Contractor: Booz Allen Hamilton

☐ **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): 9/25/2019

Anticipated Date of Updated ATO: 9/25/2022

☐ **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: Essie L. Bell

Email: Essie.Bell@faa.gov

Phone Number: 202-267-6034

COMPONENT PRIVACY OFFICER Analysis

This assessment is an update to the adjudicated PTA, dated September 26, 2018. The SOAR system is used to track grants funding applications and funding transfers between the FAA and airports across the U.S. in relation to administering the AIP and PFC programs. It is comprised of two subsystems: SOAR External (referred to as AEP) and SOAR Internal. SOAR is contractor owned and managed by Booz Allen Hamilton (under contract DTFAWA-12-D-00060). FAA Privacy finds SOAR to be a privacy sensitive system as information is obtained from members of the public and members of the DOT Federal and contract workforce. However, the PII maintained in the system consists of business contact information, userIDs, passwords and security questions/answers. The members of the public are sponsor, congressional and other aviation industry liaisons who provide business information, as appropriate. Additionally, for SOAR Internal, the TIN collected from members of the public is the business entity taxpayer ID and not the individual's Social Security number (SSN). The unauthorized access risks for SOAR are mitigated by the use of SSL encryption and no PII is included in any external SOAR reports. These risks for SOAR Internal are mitigated by the use of MyAccess authentication. There are numerous data exchanges which require MOUs currently in draft. The records in the system are maintained in accordance with the following SORN: DOT/ALL 13, Internet/Intranet Activity and Access Records, May 7, 2002 67 FR 30757. The records in the system do not have an approved NARA Records Disposition Schedule, however, there are continuing discussions between ARP and the RMO to identify appropriate records schedules.

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	Cyndi Flores, System Owner	05/19/2020
General Counsel	Christopher Andrews	10/27/2020
Information System Security Manager (ISSM)	None	None
Privacy Officer	Essie L. Bell	6/3/2020
Records Officer	Ernesto Villacarlos	01/22/2020

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

Control #	*Control Name*	*Primary PTA Question*	*Satisfied*	*Other than Satisfied*	*N/A*	*DOT CPO Notes*
AP-1	Authority to Collect	1.2 - Overview	X			AIP, which is established under chapter 471 of title 49, United States Code (U.S.C.). Records created for the purposes of account creation, logging, auditing, etc. are covered by DOT/ALL-13. DOT CPO issued a POA&M on 9/26/2018 because the then current PTA did not adequately explain the use of TIN/SSN in the system. DOT CPO authorizes the cancellation of the POA&M based on this assessment.
AP-2	Purpose Specification	1.2 - Overview	X			SOAR is the Federal Aviation Administration (FAA) system used to track grant applications and funding transfers between the DOT and airports across the United States in order to administer the Airport Improvement Program (AIP) and the Passenger Facility Charge (PFC) program. **Note**: The System Owner has submitted a change request for the input form to change the use of "personal" to "user" on the data entry form. While information is captured from members of the public, these individuals are sponsor, congressional and aviation industry liaisons who provide business related information on themselves and their respective organizations. The change in designation from "personal" to "user" does not alter the characteristic of the data collected – contact information about individuals is still considered PII. Records created for the purposes of account creation, logging, auditing, etc. are covered by DOT/ALL-13
AR-1	Governance and Privacy Program	Common Control	X			Addressed by DOT CPO.

Control #	*Control Name*	*Primary PTA Question*	*Satisfied*	*Other than Satisfied*	*N/A*	*DOT CPO Notes*
AR-2	Privacy Impact and Risk Assessment	Program Management		X		**POA&M** **Issue**: System meets eGov requirements for PIA because it collects and maintains information from members of the public. **Requirement:** submit PIA. **Timeline:** 90 days. NOTE: Most PII is collected in support of business activities, however some business entities that submit data are sole proprieters and the data submission includes TIN which may be SSN. NOTE: DOT CPO previously issued POA&M for this control in PTA adjudicated on 9/26/2018.
AR-3	Privacy Requirements for Contractors and Service Providers	3.3 - Contractor System		X		**POA&M** **Issue:** Contracts may not have appropriate Privacy language. Contractors may not be aware of their responsibilities for the protection and use of PII. **Requirement:** Update contracts to include appropriate language. **Timeline:** 365 days from PCM
AR-4	Privacy Monitoring and Auditing	Common Control	X			Addressed by DOT CPO.
AR-5	Privacy Awareness and Training	Common Control	X			Addressed by DOT CPO.
AR-6	Privacy Reporting	Common Control	X			Addressed by DOT CPO.
AR-7	Privacy-Enhanced System Design and Development	2.5 - SSN Reduction	X			DOT CPO issued a POA&M on 9/26/2018 because the then current PTA did not adequately explain the use of TIN/SSN in the system. DOT CPO authorizes the cancellation of the POA&M based on this assessment.

Control #	*Control Name*	*Primary PTA Question*	*Satisfied*	*Other than Satisfied*	*N/A*	*DOT CPO Notes*
AR-8	Accounting of Disclosures	2.7 - SORN			X	Primary records for the system are not protected by the Privacy Act.
DI-1	Data Quality	1.2 - System Overview	X			Data collected directly from individuals.
DI-2	Data Integrity and Data Integrity Board	3.4 - Security Risk Categorization			X	Activity does not constitute sharing covered by the CMA.
DM-1	Minimization of PII	2.2 – Information About Individuals	X			DOT CPO issued a POA&M on 9/26/2018 because the then current PTA did not adequately explain the use of TIN/SSN in the system. DOT CPO authorizes the cancellation of the POA&M based on this assessment.
DM-2	Data Retention and Disposal	2.11 - Records Disposition Schedule		X		See SI-12 – Information Handling and Retention
DM-3	Minimization of PII Used in Testing, Training, and Research	2.2 – Information About Individuals			X	System not used for testing, training, research.
IP-1	Consent	2.7 - SORN		X		**Issue**: Ondividuals not given an opportunity to review and understand how their PII will be used. The AEP website does not include a Privacy Act Statement (PAS). **Requirement**: Implmentat privacy policy specific to system PII collection on websites. **Timeline**: 30 days. **Note:** Consent required for collection of information necessary to create accounts covered by DOT/ALL-13. **Note:** This POA&M

Control #	*Control Name*	*Primary PTA Question*	*Satisfied*	*Other than Satisfied*	*N/A*	*DOT CPO Notes*
						was previously issued in PTA adjudicated 9/26/20. **Note**: see TR-1 and TR-2
IP-2	Individual Access	2.8 – Exemption Rule			X	Records created for the purposes of account creation, logging, auditing, etc. are covered by DOT/ALL-13
IP-3	Redress	2.7 - SORN	X			Records created for the purposes of account creation, logging, auditing, etc. are covered by DOT/ALL-13
IP-4	Complaint Management	Common Control	X			Addressed by DOT CPO.
SE-1	Inventory of PII	Common Control	X			SOAR is a privacy sensitve system. System categorization at Low Confidentiality is appropriate for the protection of PII. The Adjudicated PTA or copy of controls/POA&Ms should be included in the risk acceptance package for the system. DOT CPO recommends maintaining encryption of TIN field and records containing TIN as some may be the SSN of sole proprieters. The Adjudicated PTA should be uploaded into CSAM as evidence that the required privacy analysis for this system has been completed. **Note**: the infrastructure support plans for the system are not clearly articulated in the PTA. At the time of submission the FAA states, "SOAR has completed the migration of the SOAR-Demo web server and supporting database to the FAA Amazon Web Services GovCloud (FCS AWS GovCloud)[12] platform; however, only a SOAR test server is currently located in the cloud platform at this time." Updates to the infrastructure should be captured in the PCM for the next annual authorization. SOAR should be captured as a

[12] FCS AWS GovCloud (CSAM #2092) has an adjudicated PTA, dated 08/16/2019.

Control #	*Control Name*	*Primary PTA Question*	*Satisfied*	*Other than Satisfied*	*N/A*	*DOT CPO Notes*
						system covered by the FCS AWS GovCloud in that systems next annual authorization. The PTA should be updated not later than the next security assessment cycle and must be approved by the DOT CPO prior to the authorization decision. Component policy or substantive changes to the system may require that the PTA be updated prior to the next security assessment cycle.
SE-2	Privacy Incident Response	Common Control	X			Addressed by DOT CPO.
TR-1	Privacy Notice	2.7 - SORN			X	See IP-1
TR-2	System of Records Notices and Privacy Act Statements	2.7 - SORN			X	See IP-1
TR-3	Dissemination of Privacy Program Information	Common Control	X			Addressed by DOT CPO.
UL-1	Internal Use	2.10 - Internal and External Use		X		Information sharing agreements/MOU/other instrument required for sharing or PII between DOT/FAA systems. PII collected as professional contact information is not covered by Privacy Act but still considered information about

Control #	*Control Name*	*Primary PTA Question*	*Satisfied*	*Other than Satisfied*	*N/A*	*DOT CPO Notes*
						individual, particularly for those records connected to sole proprieterships. **POA&M** • **Issue**: Agreements required to cover PII sharing with MyAccess and NASR. **Requirement**: establish agreements/other appropriate instrument to address authorized uses of PII including retention and data protection. **Timeline**: 365 days. Records created for the purposes of account creation, logging, auditing, etc. are covered by DOT/ALL-13.
UL-2	Information Sharing with Third Parties	2.10 - Internal and External Use	X			USASpending, BTS – no PII is exchanged. Information not authorized for disclosure beyond DOT/DOT-contractors. Records created for the purposes of account creation, logging, auditing, etc. are covered by DOT/ALL-13
SI-12	Information Handling and Retention			X		**POA&M** • **Issue**: System does not have properly authorized records retention schedule; therefore records must be maintained as permanent records. **Requirement**: Submit proposed records schedule to DOT Records Officer. **Timeline**: 90 days. **Note**: POA&M previously issued in PTA adjudicated 9/26/18