U.S. Department of Transportation

Privacy Impact Assessment

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

Authorizing Official

Kevin Luey, SOAR System Owner, Office of Airports
Airports Planning and Programming
Email: Kevin.Luey@faa.gov
Phone Number: 303-342-1253

Reviewing Official

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

Executive Summary

The Office of Airports (ARP), within the Federal Aviation Administration (FAA), helps ensure a safe, efficient, and environmentally responsible national airport system that meets the needs of the traveling public, the Nation, and the world. ARP's mission is to be a world leader in creating a safe and efficient system of airports. ARP does this through the administration of airport financial assistance programs, airport planning and environmental guidance and oversight, airport engineering, design and construction standards, airport safety and operations rulemaking, and airport compliance programs. Information solicited by the System of Airports Reporting (SOAR) is collected under the authority of 49 United States Code (U.S.C.) Chapter 471, 49 U.S.C. 322 , 49 U.S.C. 40117, Public Law 115-254 FAA Reauthorization Act of 2018 and 2 Code of Federal Regulation (C.F.R.) 200.305.

In accordance with E-Government Act of 2002, the FAA developed this Privacy Impact Assessment (PIA) because SOAR collects Personally Identifiable Information (PII) from members of the public (airport owners/operators, sponsors/public agencies, air carriers, and their authorized consultants). SOAR also collects information on Department of Transportation (DOT)/FAA employees/contractors.

What is a Privacy Impact Assessment?

The Privacy Act of 1974 articulates concepts for how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The assessment is a practical method for evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed. The PIA is an analysis of how information is handled to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; ii) determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and iii) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[1]

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

Conducting a PIA ensures compliance with laws and regulations governing privacy and demonstrates the DOT's commitment to protect the privacy of any personal information we collect, store, retrieve, use and share. It is a comprehensive analysis of how the DOT's electronic information systems and collections handle personally identifiable information (PII). The goals accomplished in completing a PIA include:

- *Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk, and of options available for mitigating that risk;*
- *Accountability for privacy issues;*
- *Analyzing both technical and legal compliance with applicable privacy law and regulations, as well as accepted privacy policy; and*
- *Providing documentation on the flow of personal information and information requirements within DOT systems.*

Upon reviewing the PIA, you should have a broad understanding of the risks and potential effects associated with the Department activities, processes, and systems described and approaches taken to mitigate any potential privacy risks.

Introduction & System Overview

Within the FAA's ARP, the Office of Planning and Programming (APP) is responsible for airport planning, financial assistance tracking and administration, environmental and compliance support, and data analysis. To facilitate this work, FAA and airport stakeholders utilize the SOAR.

SOAR consists of two (2) major sub-systems: SOAR Internal and SOAR External.

SOAR Internal:

SOAR Internal is only used by internal DOT/FAA users. Internal modules cover business functions for the National Plan of Integrated Airport Systems (NPIAS), Air Carrier activity, grant administration (including Airport Improvement Program (AIP), Supplemental grants programs, Bipartisan Infrastructure Law (BIL), three COVID Relief programs, and the Passenger Facilities Charge (PFC) program). SOAR Internal also includes modules with sponsor, public agency, and Airport contact information, user information, prior year archives, reporting, SOAR issue reporting and tracking, and user notifications. ARP staff as well as various stakeholder organizations [e.g., Office of Finance and Management (AFN)], Office of Government and Industry Affairs (AGI) are authorized to access SOAR based on job function.

PII associated with SOAR Internal includes user profile information, airport owner/operator contact information and sponsor/public agency (grantee's) Tax Identification Number (TIN). The user profiles and airport contact information include name, title, organization, business email, and business phone number. For authorized users, this information is used to identify the business need for system access permissions. SOAR Internal supports FAA outreach around any of the various ARP-related responsibilities as well as FAA notifications. Sponsor/public agency information includes unique identification, such as TIN and Unique Entity Identifier (UEI), required for matching grantee name and ensuring proper payment by the financial system. SOAR Internal uses FAA's MyAccess for authentication and an internal data store for access permissions.

SOAR Internal is comprised of the following business modules:

- **Air Carrier Activity Information System (ACAIS):** ACAIS is the primary source in SOAR Internal for the viewing, editing, and addition of airport, carrier, enplanement, and cargo information. This module includes data entry, scenario generation, and statistical reporting to track the cargo and passenger landings for a given calendar year in support of the NPIAS. Reports generated include statistical reports and may contain PII (such as airport contact information).
- **National Plan of Integrated Airport Systems (NPIAS):** NPIAS determines the amount of funds with which the airport is entitled. The NPIAS module consists of statistical data entry and reporting to track the cargo and passenger landings for a given calendar year. It generates statistical reports and may contain airport contact information (such as airport data, carrier data, and business contact information).
- **Airport Improvement Program (AIP):** AIP is a grant program that supports numerous supplemental discretionary programs, three COVID-relief grants programs and BIL, as well as historical grants programs. It encompasses grants planning, processing, and funds control. The AIP module primarily 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 has completed its lifecycle. The AIP module also tracks all funding associated with a grant and its projects until the grant is closed. Grant information is retrieved by searching for non-PII data (e.g., Location ID (LOCID), NPAIS Number, Fiscal Year, or other grant attributes) from the grant search screen.
- **Passenger Facilities Charge (PFC):** PFC tracks PFC applications, associated projects and collected revenue. PFC applications are submitted by a public agency and serve as the initial request to impose passenger facility charges on airline tickets

and use funds collected for eligible projects. ARP staff receives the applications via various methods (e.g., email, regular mail, in person), and manually enter application data into SOAR.

There are nearly 400 reports associated with these modules. SOAR Internal also includes ad hoc report capability limited to internally published data sets. Reports may contain PII including contact information for federal employees (such as program manager and environmental contacts), as well as contact information for members of the public, including airport contacts.

In addition to the core modules, SOAR functional areas include sponsor/public agency Information, User Profile/Administration, Worksite, Risk Assessment, Notifications, Findings and Ideas, Sys Control, Workflow Management, and others. Of these, User Profile, Administration and Sys Control collect and/or display user specific data including name, organization, business address, business phone, and business email. The data should be business related, but the system can only validate the data format not the content or context. The sponsor/public agency information includes contact information for those entities including sponsor type, district office, congressional district, Delphi Supplier Number, and TIN and UEI numbers. A TIN is a required field captured in SOAR when a new sponsor is manually entered into the system by ARP user. The name and phone number of the airport's manager is electronically imported due to a connection with the FAA National Airspace System Resources (NASR).

PII is input into SOAR Internal by the FAA employee or contractor user or, in the case of contact information, could come from a data exchange with another system (i.e., NASR).

Airports External Portal (AEP) - SOAR External:

SOAR External (hereinafter referred to as "AEP") supports external organizations responsible for providing or confirming data. AEP modules include information provided by airports, sponsors, or their consultants about proposed and ongoing projects for potential coverage under grants programs; air carrier and cargo data upload functions supporting filing requirements by airlines and airports; and public agencies or airport provided collection and disbursement information required by the PFC program. AEP is accessed via the Internet by authorized users based on a system assigned username and user-specified 12-character password. Authorized users provide PII including name, organization, airport affiliation, business address, business phone, and business email. Authorized users can also enter contact information for the organization/airport associated with their account.

AEP is a public-facing website available at URL https://aep.airports.faa.gov (hosted securely using Secure Sockets Layer (SSL). AEP allows authorized users to access air carrier, PFC and AIP data input and reporting features relevant to their programs. External users include public agency, sponsor, airport, and air carrier users and consultants utilized by those entities.

To request an AEP account for any module/business function, the user goes to the public website above and completes a "New User Request Account" web form. On the form they specify non-FAA user (FAA users are limited to account approval/management roles), and enter required fields including name, title, business email address, country, business phone number, and business address. Prior to submitting their request, users view the previously entered data and can return to prior screens if corrections are required. This screen also includes the full text of the Privacy Act Statement (PAS), which requires acknowledgement prior to submitting the request.

Access requests are sent through two or three levels of FAA program managers depending on the module requested. The system generates an email that is sent to the email address provided to communicate request disposition and status. If approved, an email also provides the user a username and temporary password, which they must change during their first login.

Once the user has access to the system, they can perform functions related to the airport and program they represent. For example, if granted PFC access, they can enter quarterly PFC financial data for a specified airport (if more than one is permitted) by choosing that airport from a drop-down list and input revenue details for specified calendar years. AEP also provides access to reports targeted to the needs of external users.

SOAR Internal/External has data exchanges with the following internal FAA systems:

- **Adobe Sign:** SOAR exchanges the name, title, and email of air carriers, airports, sponsor/public agencies, and attorneys with Adobe Sign, using Application Program Interfaces (APIs) over Hypertext Transfer Protocol Secure (HTTPS) for the purpose of getting a grant agreement electronically signed. A Memorandum of Understanding (MOU) is part of the purchase agreement and covers this data exchange.

- **Office of Flight Standards Service:** SOAR administrators manually download a Flight Standards data file, which contains Flight Standards publicly available air taxi commercial operators contact information including name, email, address, etc. This

is published by the Office of Flight Standards Service every year and uploads to SOAR to populate Flight Standards contact data.

- **Enterprise Information Management (EIM):** EIM receives the SOAR data identified in the Alteryx Interconnect data SOAR Fields.xlsx documents to integration SOAR data with other FAA data sources using a sqlnet connection to the SOAR database through the Alteryx subsystem.

- **NASR:** SOAR pulls NASR data via an Oracle database connection including the name of an airport manager and their phone number as well as airport runway information.

- **Delphi Transfer File (DTF):** SOAR pulls non-PII accounting, grant obligation, invoice, and payment data from FAA's DTF via an Oracle Database link for the purpose ensuring accurate accounting information is maintained within SOAR. An MOU covers this data exchange.

- **Terminal Area Forecast (TAF):** A member of Airport Planning and Programming (APP-400) provides the SOAR system administrator with non-PII forecast data, including how many based airplanes at the airport, how many passengers at the airport, etc. 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.

- **Grants Notification System (GNS):** GNS receives an excel file via email from ARP to the AGI where the DOT's GNS program manually uploads the sponsor's name, which is used for Office of the Secretary of Transportation (OST) to generate grant announcements.

- **MyAccess:** SOAR uses the MyAccess system as an authentication mechanism. MyAccess sends the FAA employee and contractor user FAA contact information including email, Active Directory name to SOAR. 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. The data exchange is covered by the Common Control Provider PII Data Sharing

Agreement between AFN-AIT MyAccess and SOAR.

- **Bureau of Transportation Statistics (BTS):** The SOAR System Administrator requests non-PII 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.

- **Airport Document Management System (ADMS):** ADMS sends and receives multiple document types and thus the PII depends on which document is sent. The PII may include FAA employee/contractor, air carrier, airports, and sponsors/public agency name, email, address, phone number, etc. using HTTPS for long-term storage of SOAR documents.

- **USASpending.gov:** A public, government transparency website (external to DOT) wherein SOAR users manually transfers non-PII grant data from SOAR into USASpending.gov for the purpose of populating grant information on the website.

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template is based on the fair information practice principles (FIPPs). The FIPPs, rooted in the tenets of the Privacy Act, are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs provide a framework that will support DOT efforts to appropriately identify and mitigate privacy risk. The FIPPs-based analysis conducted by DOT is predicated on the privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v3, sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council and the Privacy Controls articulated in Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations.

Transparency

Sections 522a(e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act require public notice of an organization's information practices and the privacy impact of government programs and activities. Accordingly, DOT is open and transparent about policies, procedures, and technologies that directly affect individuals and/or their personally identifiable information (PII). Additionally, the Department should not maintain any system of records the existence of which is not known to the public.

The FAA employs multiple techniques to inform FAA employees for which the FAA collects, uses, disseminates, and retains their PII in SOAR. Access and authentication records are covered by the Privacy Act and DOT/ALL 13, *Internet/Intranet Activity and Access Records* 67 FR 30757 (May 7, 2002). All other records within SOAR are not covered by the Privacy Act, hence a SORN is not required for those records as they describe airports and are not about individuals.

Additionally, the AEP web interface provides a SOAR Privacy Act Statement (PAS) link on the Warning page (prior to log in), on the new user request form, and on the user profile page, which informs the viewer of the authority to collect their PII and how their PII will be used. This collection is in accordance with the approved Information Collection Requests (ICR) Office of Management and Budget (OMB) numbers 2120-0569 (Airports Grants Program) and 2120-0067 (Air Taxi and Commercial Operator Airport Activity Survey).

The publication of this PIA further demonstrates DOT's commitment to provide appropriate transparency regarding the handling of such information.

Individual Participation and Redress

DOT provides a reasonable opportunity and capability for individuals to make informed decisions about the collection, use, and disclosure of their PII. As required by the Privacy Act, individuals should be active participants in the decision-making process regarding the collection and use of their PII and they are provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

Users enter their PII directly through FAA approved account request forms available from the SOAR and AEP login pages. Once an account is created, users can update certain information (i.e., first name, last name, title, email address, phone number, and address) but it does not affect the existing account privileges or identification via a user profile screen. Noneditable information (such as name and organizational changes) can be corrected, after required approvals, via the SOAR System Owner or SOAR Helpdesk. Airport contact information is generally entered and updated by external users and synchronized with SOAR, although information can also be entered by SOAR users. SOAR obtains the Airport Manager information from NASR, which is the system of record for that data as well as for runway data.

TIN is relayed to SOAR users by a grantee or by consulting the System for Award Management (SAM) for the purpose of ensuring correct grantee name and financial accounting information between SOAR and the financial system of record, DOT Delphi. Discrepancies are identified through regularly occurring automated and manual comparisons

If there is a discrepancy in the TIN between SOAR and SAM, there is a way to correct it on the Sponsor page in SOAR.

From a privacy perspective, both user and non-user contact information is intended to be business information. However, provided it is properly formatted (e.g., phone number, email, TIN) the system cannot detect or prevent input of personal information.

SOAR is not a Privacy Act System of Records for the substantive records within the system, as those records relate to airport business transactions, and not individuals. However, as users authenticate individually, access and authentication records are covered under the Privacy Act. As a result, under the provisions of the Privacy Act, individuals may request searches to determine if any acces and authentication records have been added that may pertain to them. Individuals wishing to know if their access and authentication records appear in this system may inquire in person or in writing to:

Federal Aviation Administration
Privacy Office
800 Independence Ave. SW
Washington, DC 20591

Included in the request must be the following:

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

Contesting record procedures:

Individuals wanting to contest information about themselves contained in this system should make their requests in writing, detailing the reasons for why the records should be corrected to the following address:

Federal Aviation Administration
Privacy Office
800 Independence Ave. SW
Washington, DC 20591

Individuals may also use the above address to register a complaint or ask a question regarding FAA's privacy practices. If you have comments, concerns, or need more

information on FAA privacy practices, please contact the Privacy Division at privacy@faa.gov or 1 (888) PRI-VAC1.

Purpose Specification

DOT should (i) identify the legal bases that authorize a particular PII collection, activity, or technology that impacts privacy; and (ii) specify the purpose(s) for which it collects, uses, maintains, or disseminates PII.

Information solicited by the System of Airports Reporting (SOAR) is collected under the authority of 49 United States Code (U.S.C.) Chapter 471, 49 U.S.C. 322 , 49 U.S.C. 40117, Public Law 115-254 FAA Reauthorization Act of 2018 and 2 Code of Federal Regulation (C.F.R.) 200.305.

The FAA collects Name, Username, Password, User ID, Title, Company name, Business email, Fax number, Country, Business phone, Mobile phone, Pager number, Business TIN, Organization and Business address. The purpose of collecting PII is to ensure proper alignment between public agency, sponsor, or airport financial records within SOAR and the Department of Transportation financial accounting system. Also, PII identifies users to confirm the need to know and control access permissions for specific business functions and for contact information related to specific roles at airports, sponsors or public agencies.

Data Minimization & Retention

DOT should collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected.

SOAR only collects and uses the data that is required for SOAR to function and to successfully address the purposes detailed above. Records in SOAR are handled in accordance with the following National Archives and Records Administration (NARA) General Records Schedules (GRS):

NARA GRS 3.2, *Information Systems Security Records*, approved January 2023.
DAA- GRS-2013-0006-0003 covers audit logs and system access records. The records are temporary and are destroyed when business uses ceases.

NARA GRS 3.1, *General Technology Management Records*, approved November 2019.
DAA-GRS-2013-0005-0004 covers activities associated with the operations and maintenance of the basic systems and services used to supply the agency and its staff with access to computers and data telecommunications. The records are temporary and are

destroyed 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated, or superseded, but longer retention is authorized if required for business use.

The FAA Records Liaison Officer is drafting a new schedule for the substantive records in SOAR. These records are to be maintained as permanent by SOAR until the new schedule is approved by NARA.

Use Limitation

DOT shall limit the scope of its PII use to ensure that the Department does not use PII in any manner that is not specified in notices, incompatible with the specified purposes for which the information was collected, or for any purpose not otherwise permitted by law.

SOAR minimizes its data collection to meet the authorized business purpose and mission of ARP to ensure proper alignment between public agency, sponsor, or airport financial records within SOAR and the DOT financial accounting system. SOAR only shares PII via an MOU and/or PII Sharing Agreement as necessary for the effective functioning of the program.

Profile and log-in PII collected by the FAA is used only as specified by the Department's SORN DOT/ALL 13, *Internet/Intranet Activity and Access Records,* 67 FR 30757 (May 7, 2002) and is subject to the published routine uses, including:

- To provide information to any person(s) authorized to assist in an approved investigation of improper access or usage of Department of Transportation (DOT) computer systems;
- To an actual or potential party or his or her authorized representative for the purpose of negotiation or discussion of such matters as settlement of the case or matter, or informal discovery proceedings;
- To contractors, grantees, experts, consultants, detailees, and other non-DOT employees performing or working on a contract, service, grant cooperative agreement, or other assignment from the Federal government, when necessary to accomplish an agency function related to this system of records; and
- To other government agencies where required by law.

The Department has also published 15 additional routine uses applicable to all DOT Privacy Act systems of records, including this system. These routine uses are published in the Federal Register at 75 FR 82132, December 29, 2010, and 77 FR 42796, July 20, 2012,

under "Prefatory Statement of General Routine Uses." Available at Uniform Resources Locator (URL) https://www.transportation.gov/individuals/privacy/privacy-act-system-records-notices.

Data Quality and Integrity

In accordance with Section 552a(e)(2) of the Privacy Act of 1974, DOT should ensure that any PII collected and maintained by the organization is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in the Department's public notice(s).

Information in SOAR is collected directly from FAA employees, contractors, and members of the public. They complete the form and verify that all the data elements are correct and thus it is assumed to be accurate. SOAR data input screens and data interconnections check data to ensure well-formatted data for information such as name, city, state, zip, phone, email, and TIN, which constitute the PII data in SOAR. Erroneous contact information and/or user profile data is updated as errors are uncovered through normal operations (e.g., returned emails) or user-initiated actions (failure to reach a contact at number provided). TIN is currently manually validated with Delphi through the grant obligation process.

Security

DOT shall implement administrative, technical, and physical measures to protect PII collected or maintained by the Department against loss, unauthorized access, or disclosure, as required by the Privacy Act, and to ensure that organizational planning and responses to privacy incidents comply with OMB policies and guidance.

The FAA protects PII with reasonable security safeguards against loss or unauthorized access, destruction, usage, modification, or disclosure. These safeguards incorporate standards and practices required for federal information systems under the Federal Information Security Management Act (FISMA) and are detailed in Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, dated March 2006, and the National Institute of Standards and Technology Special Publication (NIST) 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations,* dated September 2020 (includes updates as of Dec. 10, 2020).

These safeguards include an annual independent risk assessment of SOAR to test security processes, procedures and practices. The system operates on security guidelines and standards established by NIST and only FAA personnel with a need to know are authorized to access the records in SOAR. All data in-transit between a user's browser

and SOAR web server is encrypted and access to electronic records is controlled by Personal Identity Verification (PIV) and Personal Identification Number (PIN) and limited according to job function. Additionally, FAA conducts an annual cybersecurity assessment to test and validate security process, procedures and posture of the system. Based on the security testing and evaluation in accordance with the FISMA, the FAA issues SOAR an on-going authorization to operate.

Accountability and Auditing

DOT shall implement effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that the Department is complying with all applicable privacy protection requirements and minimizing the privacy risk to individuals.

FAA Order 1370.121B, *"FAA Information Security and Privacy Program & Policy,"* implements the various privacy requirements of the Privacy Act of 1974 (the Privacy Act), the E-Government Act of 2002 (Public Law 107-347), DOT privacy regulations, Office of Management and Budget (OMB) mandates, and other applicable DOT and FAA information and information technology management procedures and guidance.

DOT implements effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that the Department is complying with all applicable privacy protection requirements and minimizing the privacy risk to individuals.

In addition to these practices, the FAA consistently implements additional policies and procedures especially as they relate to the access, protection, retention, and destruction of PII. Federal employees/contractors who work with SOAR are given clear guidance about their duties as related to collecting, using, and processing privacy data. Guidance is provided in mandatory annual security and privacy awareness training and in FAA Order 1370.121B. The FAA also conducts periodic privacy compliance reviews of SOAR as related to the requirements of OMB Circular A-130, "*Managing Information as a Strategic Resource*."

Responsible Official

Kevin Luey
SOAR System Owner
Management Analyst, Office of Airports, Airports Planning and Programming

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN MARIE GORMAN
Digitally signed by KARYN MARIE GORMAN
Date: 2024.10.21 11:51:27 -04'00'