U.S. Department of Transportation

Privacy Impact Assessment
Federal Aviation Administration (FAA)
Office of Airports (ARP)
Airport Compliance Application Suite (ACAS)

Responsible Official

Michael Helvey
Director, Office of Airports Compliance and Management Analysis
michael.helvey@faa.gov

Reviewing Official

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

Executive Summary

The Federal Aviation Administration's (FAA) Airport Compliance Activity Suite (ACAS) consists of three sub-system enterprise-level applications used by Federal employees, contractors, and external airport entities to gather airport financial data using the Certification Activity Tracking System (CATS), and address compliance issues in the United States (U.S.) Airports using the Airport Compliance Division Compliance Database (ACODB) and provides a publicly accessible archive of the outcome of complaints filed against airports using the Part 16 Decision Database (Part 16). The ACAS system is authorized under 44 United States Code (U.S.C.) Sections 106(t), 3101, 40101, 42121, and 44701 Section 341, 510, 1210, Federal Aviation Reauthorization Act of 1996; Section 180, FAA Reauthorization Act of 2018.

The FAA published this updated Privacy Impact Assessment (PIA) for ACAS in accordance with Section 208 of the E-Government Act of 2002 because a new application, Part 16 Case Management System (CMS), was added and to inform the public that the system is no longer a Privacy Act system of records and to update the System of Records Notices (SORN) section of the PIA. ACAS processes Personally Identifiable Information (PII) from members of the public, including public and private airports owners/airport employees, authorized airport representatives, sponsors, legal counsel, and complainants.

What is a Privacy Impact Assessment?

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

[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

The Office of Airports Compliance and Management Analysis (ACO) within the Office of Airports (ARP) operates all subsystems within ACAS to allow the ACO to track informal compliance issues, archive Part 16 decisions, and administer the Airport Financial Reporting Program.

ACAS is a non-Privacy Act web-based application, and different components are accessible to members of the public and FAA employees/contractors. ACAS is comprised of the following four components, all supporting the ACO mission:

1. Certification Activity Tracking System (CATS) – Central location for the gathering and dissemination of congressionally mandated airport financial information that offers publicly available read-only information. The information available to the public contains information such as airport name, location ID, state, FAA region, and year filed within the "View and Airport Financial Report" section of CATS.
2. Airport Compliance Division Compliance Database (ACODB) – Airport sponsor filing and complaint system.
3. Part 16 Decision Database (Part 16) – Publicly accessible, read-only archive of the outcome of complaints filed alleging non-compliance of a federally funded airport.

4. Part 16 Case Management System (CMS) – Tracking and maintaining the archive of Part 16 investigations and actions internal to ACO.

The four subsystems are fully described below:

1. CATS Subsystem

CATS is a web-based module for gathering and disseminating congressionally mandated airport financial information. United States (U.S.) private and public airport owners are required to submit annual financial reports using FAA Form 5100-126, *Financial Government Payment Report* and FAA Form 5100-127, *Operating and Financial Summary Report* through the Airport Financial Reporting Program Website at Uniform Resource Locator (URL) https://cats.airports.faa.gov.

If an airport fails to submit its reports, the FAA issues a letter notifying the airport of the overdue report. If the reports are not received within 30 days of the letter, the FAA may withhold future entitlement and discretionary Airport Improvement Program (AIP) grant awards. The FAA may also suspend payments on existing grants.

2. ACODB Subsystem

ACODB is available only within the FAA network and accessible only to FAA employees and contractors. It is designed for FAA ARP employees to research, record, and report information related to potential compliance issues at U.S. airports. These records track possible violations of federal obligations by airport sponsors. FAA employees and contractors may use ACODB to track compliance issues before filing a Part 16 complaint. ACODB is used to record correspondence, documentation, and findings related to informal complaints. The Office of Airports regional and district offices typically intake informal complaints when a complainant has an issue with the airport sponsor and files with the ARP regional offices by email, mail, or telephone. The substance of the complaint concerns an airport, not an individual. There is no specific set of required information that must be included in the complaint when it is filed. The type of PII contained in complaints generally includes the complainant's name, business address, business telephone number, business email address, and the airport's authorized representative's name and contact information.

In this capacity, ACODB is a mechanism for ACO to resolve compliance issues before they become subject to legal enforcement action. ACODB is also used as a historical archive to record the decisions rendered on informal complaints. Records include the airport's point of contact and sponsor names.

The ARP regional and district offices typically record issues reported by airport users and questions about the airport, especially those related to the grant assurances. If an informal complaint is filed, the FAA employee handling the issue sends an electronic

letter to the airport describing the alleged complaint and uploads a copy of the letter into ACODB. The ACO employee or an appropriate FAA employee within the region investigates the issue. The regional FAA employee may also conduct a site visit and record details of the airport visit, which they later manually enter into ACODB.

3. Part 16 Decision Database (Part 16) Subsystem

The Part 16 subsystem is a publicly accessible, read-only archive at URL https://part16.airports.faa.gov. This database contains summaries of the outcomes of complaints filed by individuals (complainants) who are directly and substantially affected by alleged non-compliance of a federally funded airport. The Part 16 database also includes FAA administrative decisions, Part 16 Director's Determinations, Final Agency Decisions, and appeals court rulings. All documents are saved as Adobe Acrobat Portable Document Format (PDF) and are accessible to any member of the public. The PII contained in Part 16 includes the complainant and/or respondent's name and case docket number.

4. Part 16 Case Management System (CMS) Subsystem

Since 2021, Part16 CMS tracks and maintains a history of Part 16 cases from docketing through the pleadings, FAA issuance, and, if applicable, appeals phases. It replaced ACO's older Part 16 tracking spreadsheet and is available at URL https://acocms.airports.faa.gov. Part 16 CMS also calculates and sends due-date notifications to the assigned staff during each phase and provides status reports for ongoing Part 16 investigations. Additionally, this application provides high-level analytics and charts, which inform management decision-making and create efficiency and productivity measurements.

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[2].

[2] https://csrc.nist.gov/publications/detail/sp/800-53a/rev-5/final

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 ACAS is a privacy-sensitive system because it maintains, collects, uses, and disseminates PII from public and private airport owners/airport employees/authorized airport representatives/sponsors, complainants/respondents, and legal counsel for legal communications and enforcement of airport grant obligations. The substantive information in ACAS is not subject to the Privacy Act because the records are not about individuals (in their individual capacity) and are not routinely retrieved by PII. Records are retrieved using the Airport Locator Code (LOC) or docket number. Policies, procedures and practices for information storage, data use, access, notification, retention, and disposal are described in this PIA.

Records for login credentials, audit trails, and security monitoring for FAA employees and contractors who are part of the ACAS program and/or manage the system are subject to the Privacy Act and covered by SORN DOT/ALL 13, *Internet/Intranet Activity and Access Records* 67 FR 30757 (May 7, 2002).

The publication of this PIA demonstrates the FAA's commitment to providing appropriate transparency into the ACAS system.

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 with reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

As mentioned, ACAS is not subject to the Privacy Act because the records are not about individuals (in their individual capacity) and are not routinely retrieved by PII. Records are retrieved using Airport LOC or docket numbers.

If changes to an individual record are required in any ACAS subsystems, the individual must contact the FAA compliance administrator via the contact feature listed on the application's website. In this instance, the record could be retrieved with PII, but it is still about the airport, not the individual. For policy and accounting questions, the individual may reach the Airport Compliance Division at (202) 267-5879 or (202) 493-4604.

CATS: Airport sponsors/representatives may contact the FAA through the CATS *User Support by Email* selection at URL https://cats.airports.faa.gov/contactus.cfm on the CATS opening page for helpdesk requests to include user deletions, registration, data entry difficulties, and other general financial questions. CATS administrators are FAA employees and contractors who perform deletions and confirmations of airport users within the system. FAA ACO ensures accountability and data integrity by strictly limiting administrator data input or amendments to the airport's reports unless expressly permitted.

ACODB: This subsystem is only available within the FAA network and is not publicly accessible. The ACO employees and contractors use ACODB to research, record, and report information primarily related to potential compliance issues at U.S. airports.

Part 16: This subsystem is a publicly accessible, read-only archive of complaint outcomes, which is available at URL https://part16.airports.faa.gov/. Complainants who are directly and substantially affected by alleged noncompliance with federal requirements at a federally funded airport can submit a complaint to the FAA (through a different system) against public and private federally assisted airports. All documents are saved within the archive as Portable Document Formats (PDFs) and accessible to the public.

Part 16 CMS: This subsystem is only available within the FAA network at URL https://acocms.airports.faa.gov and is not publicly accessible. ACO tracks and records the procedural history of each Part 16 case. This application also offers a reporting system with advanced analytics and sends due date notifications to the staff assigned to each case.

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.

Congress authorized the FAA Administrator to develop systems and/or tools to support the filing of airport financial records, tracking of airport compliance issues, and the retention of Part 16 complaints. ACAS addresses the unique demands of the FAA's workforce and operates under the following authorities:

- ***49 U.S.C. 106(t)*** ***(Office of Whistleblower Protection and Aviation Safety Investigations)*** establishes in the Federal Aviation Administration the Office of Whistleblower Protection and Aviation Safety Investigations to receive complaints and information submitted by employees of persons holding certificates issued under *Title 14, Code of Federal Regulations* and employees of the Agency concerning the possible existence of an activity relating to a

violation of an order, a regulation, or any other provision of Federal law relating to aviation safety.

- ***44 U.S.C. 3102*** ***(Transportation)*** authorizes the head of each Federal agency to establish and maintain an active, continuing program for the economical and efficient management of the records of the agency.

- ***49 U.S.C. 40101*** ***(Economic Regulation)*** establishes the Secretary of Transportation shall consider the following matters, among others, as being in the public interest and consistent with public convenience and necessity: assigning and maintaining safety as the highest priority in air commerce; preventing deterioration in established safety procedures, recognizing the clear intent, encouragement, and dedication of Congress to further the highest degree of safety in air transportation and air commerce, and to maintain the safety vigilance that has evolved in air transportation and air commerce and has come to be expected by the traveling and shipping public.
- ***49 U.S.C. 42121*** **(*Protection of Employees Providing Air Safety Information)*** A holder of a certificate under section 44704 or 44705 of this title, or a contractor, subcontractor, or supplier of such holder, may not discharge an employee or otherwise discriminate against an employee with respect to compensation, terms, conditions, or privileges of employment because the employee (or any person acting pursuant to a request of the employee) … provided information relating to any violation or alleged violation of any order, regulation, or standard of the Federal Aviation Administration or any other provision of Federal law relating to aviation safety under this subtitle or any other law of the United States.
- ***49 U.S.C. 44701*** ***(Promoting Safety)*** the Administrator of the Federal Aviation Administration shall promote safe flight of civil aircraft in air commerce by prescribing— minimum standards required in the interest of safety for appliances and for the design, material, construction, quality of work, and performance of aircraft, aircraft engines…and to examine and report on the inspecting, servicing, and overhauling; regulations required in the interest of safety… and regulations and minimum standards for other practices, methods, and procedure the Administrator finds necessary for safety in air commerce and national security.

- ***FAA Reauthorization Act of 2018* (Section 180)** - The Regional Administrator for that region shall designate an individual to be the Regional Ombudsman for the region to serve as a regional liaison with the public, including community groups, on issues regarding aircraft noise, pollution, and safety; make recommendations to the Administrator for the region to address concerns raised by the public and improve the consideration of public comments in decision-making processes; and be consulted on proposed changes in aircraft operations affecting the region, including arrival and departure routes, in order to minimize environmental impacts, including noise.

ACAS, and its subsystems collect the following information as required by SORN DOT/ALL 13, *Internet/Intranet Activity and Access Records* 67 FR 30757 (May 7, 2002) to create ACAS accounts, to provide access to the system, and to manage the program. ACAS collects names, FAA email addresses, FAA telephone numbers, usernames, and passwords from FAA employees and contractors. It collects name, email address, username, and password information from public and private airport owners and airport employees.

The collected PII is not routinely used for any other purpose.

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.

FAA personnel collect and maintain the minimum amount of information from individuals to support the FAA's airport compliance programs. Records for the system are handled according to the following National Archives and Record Administration (NARA) General Retention Schedules (GRS).[3]

Operational and financial summary and financial government payment records are covered under NI-237-10-007, *Compliance Activity Tracking System*, approved October 22, 2009. These records are cutoff at the end of the fiscal year the information is received and verified, and all review or trend analysis activity is completed. They are destroyed 10 years after the cutoff date.

System access records are covered under GRS 3.2, *Information Systems Security Records*, item 030, approved January 2023. These records are temporary and are destroyed when business use ceases.

[3] General retention schedules are used by the FAA to determine how long to maintain an individual's records and when to delete the individual's records and to promote consistent retention practices.

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.

ACAS limits the collection of PII to only the PII necessary to conduct the required business processes. The FAA does not use the PII, including names (airport manager, employee, POC, company/organization/airport, complainant, and respondent), business email addresses, business/personal phone numbers, business/airport addresses, digital signatures, and Airport Identification (LOCID) information for any other purpose. The system does not retrieve records using personal identifiers and is not a Privacy Act system of records.

However, access and authentication records within ACAS are handled in accordance with SORN DOT/ALL 13, *Internet/Intranet Activity and Access Records* 67 FR 30757 (May 7, 2002). 2002). In addition to other disclosures generally permitted under 5 U.S.C. §552(a)(b) of the Privacy Act, all or a portion of the records or information contained in the system may be disclosed outside DOT as a routine use pursuant to 5 U.S.C § 552a(b)(3) as follows:

- To provide information to any person(s) authorized to assist in an approved investigation of improper access or usage of DOT computer systems.

The Department has also published 17 additional routine uses that apply 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, 77 FR 42796, July 20, 2012, and 84 FR 55222, October 15, 2019 under "Prefatory Statement of General Routine Uses."

Finally, the FAA periodically reviews the collection and use of PII through its annual review of this PIA and a Privacy Threshold Analysis.

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).

ACAS collects, uses, and retains data that is relevant and necessary for the purpose for which it was collected. Members of the public (public and private airport owners, airport employees, authorized airport representatives, and complainants) who have PII in the system are responsible for ensuring that the data that they provide is correct. When they create a report or file a complaint, they can validate or edit the information they have entered prior to submitting. When PII is collected directly from the individual, the individual is responsible for ensuring the accuracy of the information being provided.

ACAS is a web-based system, and different components are accessible to members of the public, FAA employees and contractors.[4] Specifically, Airport sponsors and representatives may contact the CATS *User Support by Email* selection at URL https://cats.airports.faa.gov/contactus.cfm on the opening page for helpdesk requests, including, but not limited to user deletions, registration, data entry difficulties, and other general financial questions.

For ACODB and Part 16, the websites are frequently used by FAA ARP employees, aviation attorneys, and members of the public and can be used to provide information and/or make general requests.

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 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 the ACAS system 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 ACAS. All data in transit and at-rest is encrypted. Access to records in the system is controlled by use of a Personal Identity Verification (PIV) card, and use of a Personal Identification Number, and limited according to job function. Additionally, FAA conducts annual cybersecurity assessment to test and validate the security processes, procedures, and posture of the system. Based on security testing and evaluation in accordance with the FISMA, the FAA issues ACAS an ongoing authorization to operate.

[4] CATS and Part 16 (Decision Database) are available to the public and FAA employees and contractors; ACODB and the Part 16 CMS are restricted to FAA employees and contractors only.

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.

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

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

In addition to these practices, the FAA will implement additional policies and procedures as needed, as they relate to the access, protection, retention, and destruction of PII. Federal employees and contractors who work with ACAS receive clear guidance on their duties related to collecting, using, and processing privacy data. Guidance is provided through mandatory annual security and privacy awareness training and FAA Order 1370.121. The FAA conducts periodic privacy compliance reviews of ACAS in accordance with the requirements of OMB Circular A-130, *Managing Information as a Strategic Resource*.

Responsible Official

Michael Helvey

System Owner
Director, Airport Compliance and Management Analysis Division (ACO-1)

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN MARIE GORMAN
Digitally signed by KARYN MARIE GORMAN
Date: 2026.05.04 16:07:17 -04'00'