U.S. Department of Transportation

Office of the Secretary (OST)

Office of Aviation Consumer Protection (C-70)

Privacy Impact Assessment
Aviation Complaint, Enforcement, and Reporting System (ACERS)

Responsible Official

Kimberly Graber
Deputy Assistant General Counsel, Business Owner, OST/OGC
Kimberly.Graber@dot.gov

Approving Official

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

Executive Summary

The Office of Aviation Consumer Protection (OACP/C-70) is part of the Office of the General Counsel (OGC) within the Department of Transportation (DOT or the Department). OACP has broad authority under 49 U.S.C., Subtitle VII, to investigate and enforce consumer protection and civil rights laws and regulations related to air transportation. OACP is responsible for enforcing the Department's aviation consumer protection requirements. ACERS is a newly modernized web-based system[1] that is used by OACP management, attorneys, and travel industry analysts. The system is primarily used to monitor complaints related to individual airlines and air travel companies and to determine the extent to which these entities are in compliance with federal aviation civil rights and consumer protection regulations. It is also used to determine when to conduct investigations and/or enforcement actions.

OACP is publishing this Privacy Impact Assessment (PIA) in accordance with the E-Government Act of 2002 because the office receives, uses, and maintains Personally Identifiable Information (PII) from members of the public. ACERS may also include limited PII on OACP personnel and 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—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.[2]

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:

[1] ACERS was formerly known as the Consumer Complaints Application (CCA). ACERS contains the same information as CCA and includes new updated features that are addressed in this PIA.

[2] 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).

- *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 Aviation Complaint, Enforcement and Records System (ACERS) is managed by the Office of Aviation Consumer Protection (OACP/C70). OACP is responsible for enforcing the Department's aviation consumer protection requirements.

ACERS is a modernized web-based system using the Salesforce platform that is used by OACP to receive complaints and inquiries from consumers who experience air travel service problems or are seeking more information about air travel-related issues. [3] All complaints/comments are entered in the system, including complaints (primarily) submitted directly by consumers via the Air Travel Service Complaint or Comment Form on OACP's website located at airconsumer.dot.gov/complaint/form.[4] A limited number of complaints are submitted via telephone and letter submissions and are uploaded into the system by OACP administrative staff.

ACERS is used primarily to monitor complaints related to individual airlines and air travel companies. In addition, it is used to determine the extent to which these entities are in compliance with federal aviation civil rights and consumer protection regulations. The system is used to provide/exchange information to aviation industry personnel and to members of the public on consumer protection matters, as well as to track statistics on flight delays, over sales, baggage problems, tarmac delays, and other air travel consumer protection covered areas. ACERS is also used to determine when to conduct investigations and/or enforcement actions.

[3] ACERS encompasses what was formerly the bifurcated system containing the Consumer Complaints Application (CCA) and the Case Tracking Management System (CTMS). The system was modernized, and the two applications were combined as ACERS.

[4] The form has an OMB Control Number (2105-0568, expires 5/31/25) that will be/was updated to include the new information contained in ACERS.

The type of information requested on OACP's legacy (CCA) online form included the complainant's name, address, phone number (including area code), e-mail address, and name of the airline or company about which the individual is complaining, flight date and flight itinerary (where applicable) of a complainant's trip. Information in ACERS also includes the country of residence, whether the trip involved a flight through the US or a US territory, and the passenger's arrival/departure airports. The ACERS complaint process allows for guided input and contains a series of radio buttons associated with the specific nature about which the consumer is complaining (e.g., disability, refunds, flight cancellations). An air consumer can also create a narrative containing specific details about their complaint.

ACERS allows a consumer to upload documents, in which case some consumers may choose to enter unsolicited PII (e.g., social security number). The complaint form includes the following statement: "Please remove or obscure sensitive personal information from your documents before uploading, including your social security number, personal financial data, and credit card numbers."

If PII is entered in the consumer's complaint description, ACERS is set up to automatically identify certain information in the "Possibly Contains PII" field (e.g., credit card number). OACP is also able to create a report that personnel can review for PII to ensure that information remains protected (e.g., in the case of a FOIA request).

PII may be retained in a case or project record if it is included in a narrative or document pertaining to the case or project, but no PII is solicited via those methods.

ACERS also allows OACP personnel to enter, update, review, analyze and manage information regarding projects and enforcement cases. Additionally, OACP can run a variety of reports using the system, included reports to Congress and General Accounting Office (GAO). Among other things, the search function within the application allows OACP to access records by case/project status, case/project name, case/project description, subject matter area, statue/rule and account records (e.g., airline personnel, complaint submitter). Authorized contractor personnel have access to ACERS for purposes of assisting OACP personnel with tasks such as running reports, regular system operations and maintenance, and minor development-related tasks.

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[5], sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council and the Privacy Controls articulated in Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations[6].

Transparency

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

Information is collected in the Air Travel Service or Complaint Form, OMB Control number 2105-0568 and may include the following information: Complainant's name, address, phone number (including area code), e-mail address, name of the airline or company about which the individual is complaining, flight date and flight itinerary (where applicable) of a complainant's trip, country of residence, whether the trip involved a flight through the US or a US territory, and the passenger's arrival/departure airports.

DOT and OACP System of Records Notices (SORNs) provide transparency about privacy practices regarding the collection, use, sharing, safeguarding, maintenance, and disposal of information about individuals covered under the Privacy Act of 1974, as amended. Because consumer information stored in ACERS may be retrieved by consumer name, phone number, physical address, and/or email address, the information is covered by System of Records Notice (SORN) DOT/OST 102 - Aviation Consumer Complaint Application (CCA) Online System - 84 FR 2663 – February 7, 2019. DOT/OST 102 claims an exemption for "Investigatory material compiled for law enforcement purposes other than criminal law enforcement," pursuant to 5 U.S.C. 552a(k)(2), this system is exempt from 5 U.S.C. 552a(d). For more information, see DOT/OST 102 Privacy Act Exemptions Final Rule - 84 FR 67671, December 11, 2019.

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

OACP may also retrieve system records/information/reports in ACERS by case/project status, case/project name, case/project description, case/project number, subject matter area, and statue/rule. Records for an individual complainant are generally retrieved using their name or an OACP assigned case number.

The publication of this PIA further demonstrates DOT's commitment to provide appropriate transparency into ACERS IT system. Information on the Department's privacy program may be found at www.transportation.gov/privacy.

Individual Participation and Redress

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

An air consumer or their representative (e.g., attorney, disabled passenger's relative) directly input the personal information, including PII, into ACERS via the online consumer complaint form guided input process. Air carriers and air travel companies' responses to consumer complaints are also loaded into ACERS. Additional documents and information submitted by covered entities in response to OACP's requests related to regulated areas, investigations, and/or enforcement actions are uploaded into ACERS. After information is uploaded into ACERS by a complainant/commenter or their representative, that individual cannot access the system to correct or amend the information. Any changes to ACERS records must be made by authorized OACP personnel and/or IT-service contractors using the "Records Access Procedure" described below.

Under the provisions of the Privacy Act, individuals may request searches of agency records to determine if any added records pertain to them.

Records Access Procedure: Individuals wishing to know if their records appear in this system may inquire in writing to:

Agency Contact Information: airconsumer2@dot.gov (preferred)

Or

Office of Aviation Consumer Protection
U.S. Department of Transportation
1200 New Jersey Avenue, SE
Washington, DC 20590

The request must include the following information:

- Name of the SORN (Aviation Complaint, Enforcement and Records System)
- Individual or Individual Representative's Name
- Mailing address
- Phone number and/or email address
- A description of the records sought, and if possible, the location of the records
- A signed attestation of the individual's identity or, in the case of an individual representing a complainant, a consent form or a signed document attesting that that individual is authorized to represent the complainant.

Contesting Record Procedures: Individuals seeking to contest information about them that is contained in the ACERS should make their request in writing, detailing the reasons their records must be corrected and addressing their letter to the following address:

Agency Contact Information: airconsumer2@dot.gov (preferred)

Or

Office of Aviation Consumer Protection
U.S. Department of Transportation
1200 New Jersey Avenue, SE
Washington, DC 20590

Additional information about the Department's privacy program may be found at https://www.transportation.gov/privacy-program. Individuals may also contact the DOT Chief Privacy Officer at privacy@dot.gov.

Purpose Specification

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

The Department's Office of Aviation Consumer Protection (OACP) has broad authority under 49 U.S.C., Subtitle VII, to investigate and enforce consumer protection and civil rights laws and regulations related to air transportation. The information collection continues to further the objectives of 49 U.S.C. § 41712, § 40101, § 40127, § 41702, and § 41705 to protect consumers from unfair or deceptive practices, to protect the civil rights of air travelers, and to ensure safe and adequate service in air transportation.[7]

ACERS data will be used by OACP consistent with the purposes for which it was collected as described in the SORNs for DOT/OST 102—*Aviation Consumer Complaint Application Online System of Records (updated),* 84 FR 2662, February 7, 2019.

[7] The provisions cited above can be found at https://www.law.cornell.edu/uscode/text/49/subtitle-VII/part-A/subpart-ii/chapter-417 and https://www.law.cornell.edu/uscode/text/49/subtitle-VII/part-A/subpart-i/chapter-401.

ACERS is the primary source of information that OACP uses to receive complaints and inquiries from consumers who experience air travel service problems. ACERS is also used for OACP to obtain information about air travel-related issues, as well as to determine when to conduct investigations and/or enforcement actions.

Data Minimization & Retention

DOT should collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected. DOT should retain PII for only if necessary to fulfill the specified purpose(s) and in accordance with a National Archives and Records Administration (NARA)-approved record disposition schedule.

ACERS receives PII and uses it to process informal complaints/inquiries from members of the public. OACP has limited its informational request to that necessary to meet its program and administrative monitoring and enforcement activities.

Data uploaded into ACERS is controlled and retained by authorized OACP analysts/attorneys and authorized IT-service contractors.

The legacy (CCA) system of records is being revised[8] and the records are kept indefinitely until a record retention schedule for ACERS is approved by the National Archives and Records Administration (NARA). OACP is working with the Department's records officer to update the system of records.

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.

ACERS receives PII and uses it to process informal complaints/inquiries from members of the public. OACP only allows authorized personnel to add, delete, or revise information, and PII within ACERS. Authorized contractor personnel have access to ACERS for purposes of assisting OACP personnel with tasks such as running reports, regular system operations and maintenance, and minor development-related tasks. OACP has limited its informational request to that which is necessary to meet its program and administrative monitoring, investigation, and enforcement activities.

Records covered under DOT/OST 102—*Aviation Consumer Complaint Application Online System of Records (updated),* 84 FR 2662, February 7, 2019, may be disclosed outside of DOT as a routine use pursuant to 5 U.S.C. § 552a(b)(3). The system receives and is used to process informal complaints and assist OACP in tracking statistics on covered areas such as flight delays,

[8] Civil Aeronautics Board, Request of Authority to Dispose of Records, July 25, 1975.

oversales, baggage problems, and consumer complaints. Additional routine uses for this system can be found in the Published Notice.

The types of record disclosures, including routine uses, are also fully articulated in the citations included in the *"Transparency"* section, above.

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).

The information being gathered is inputted directly from the consumer or consumer's representative (e.g., family member, attorney) filing the complaint/comment.

OACP receives information via a guided input online complaint form. The information is inputted directly by an individual or their representative. There is no human interface during the data transfer from the online consumer complaint form into ACERS, which eliminates the possibility of human error possibly impacting the quality of the data.

Further, OACP only allows authorized personnel to add, delete, or revise information within ACERS. Authorized contractor personnel have access to ACERS for purposes of assisting OACP personnel with tasks such as running reports, regular system operations and maintenance, and minor development-related tasks. This helps preserve data quality and greatly reduces the opportunity for the quality or integrity of the data to be compromised.

Security

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

OACP protects PII with reasonable security safeguards against loss or unauthorized access, destruction, usage, modification, or disclosure. These safeguards incorporate standards and practices required for federal information systems under the Federal Information Security Management Act (FISMA) and are detailed in Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information Systems, dated March 2006, and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, dated April 2013.

ACERS implemented specific administrative, technical, and physical measures to protect PII against loss, unauthorized access, or disclosure. Authorized OACP personnel and IT-service contractors can only access the internal interfaces via DOT's network using their Personal Identity Verification (PIV) card. Personnel receive guidance on their duties as they relate to collecting, using, processing, and securing PII. This includes mandatory annual security and privacy awareness training.

ACERS has a privacy/security incident response plan in place which includes procedures for detection of a privacy/security incident, remediation and response if one occurs, and notification where appropriate to protect and inform impacted individuals.

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.

ACERS system audit logs are analyzed for suspicious or unusual activity. Only authorized system, database, and application administrators have rights sufficient to legally access audit logs based on their roles in ACERS.

The Fair Information Practice Principles (FIPPs) are followed for the protection of information maintained in the system. Policies and procedures are consistently applied, especially as they relate to protection, retention, and destruction of records.

The ACERS system owner is responsible for ensuring information system security awareness training is provided to new employees automatically (and re-assigned annually) and to OACP employees and contractors with access to the program as required by DOT policies. The ACERS business owner will assist the system owner as needed.

The DOT Office of Standards and Technology Chief Information Officer documents and monitors individual information system security training activities, including basic security awareness training and specific information system security training. DOT Security Awareness Training is administered and maintained through DOT Learns. OACP conducts regular periodic security and privacy compliance reviews for ACERS consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*.

Responsible Official

Kimberly Graber
Deputy Assistant General Counsel, Business Owner, OST/OGC
Kimberly.Graber@dot.gov

Approving Official

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