U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration (FAA)

Office of Aviation Safety (AVS)

iTRAK

Responsible Official

Edward Cardenas
Email: edward.cardenas@faa.gov
Phone Number: 571-383-4162

Reviewing Official

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

Executive Summary

The Federal Aviation Administration (FAA) is authorized to conduct evaluations of safety complaints under 49 USC Chapter 447, and Title 49 U.S.C. Section 40113.[1] To achieve this mission, the Office of Aviation Safety (AVS), Special Emphasis Investigations Team (SEIT) developed iTRAK. iTRAK is used by SEIT to conduct analysis as it relates to the evaluation of safety complaints, which may lead to formal investigations of safety violations.

In accordance with Section 208 of the E-Government Act of 2002, the FAA is publishing this Privacy Impact Assessment (PIA) since iTRAK collects and maintains Personally Identifiable Information (PII) on members of the public such as complainants, airmen, aircraft owners, or other individuals involved in the investigation, as part of the safety complaint evaluation process.

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:

- *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;*

[1] FAA Order 2150.3C and FAA Order 8900.1Aallow for SEIT employees to execute the roles and responsibilities of FAA Aviation Safety Inspectors (ASI) in evaluating safety complaints.
[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).

- *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 FAA SEIT utilizes iTRAK to collect, store, and conduct analysis as it relates to the evaluation of safety complaints, which may lead to formal investigations of safety violations. FAA Order 2150.3C and FAA Order 8900.1A, as applicable, allow for the creation of SEIT to execute the roles and responsibilities of FAA Aviation Safety Inspectors in the conducting of investigations authorized under 49 U.S.C. Chapter 447 and Title 49 U.S.C. Section 40113.

Safety Complaint Evaluation Process

SEIT receives safety complaints, via email or letters by U.S. postal mail, for evaluation. Additionally, SEIT may receive safety complaints for evaluations through referrals from other FAA offices[3] or other federal agencies. The complaints that are received may include attachments that are supporting documentation pertaining to the safety complaint. SEIT processes complaints pertaining to the following subject areas:

- Illegal charter operations;
- FAA hotline complaints;
- Whistleblower complaints;
- FAA designee operations;
- Suspected unapproved parts; and
- Law enforcement assistance and other matters handled by the AVS Flight Standards Service.

Any complaint received may contain the complainant's name, mailing address, email address, telephone number, subject of complaint, and description of the complaint.

Once a complaint is received, a manager assigns the case to a SEIT employee for evaluation. The SEIT employee accesses iTRAK with their username and password, opens a case, and

[3] Audit and Evaluation (AAE), Security and Hazardous Materials Safety (ASH), Office of Aerospace Medicine (AAM) and Flight Service District Office (FSDO).

iTRAK generates a case number that is used to track the case. The SEIT employee then manually enters the following information into iTRAK:

- Description of the request (free text field limited to 500 characters);
- Brief summary of the request (free text field);
- Type of investigation (i.e. law enforcement, support, illegal charter, aircraft registry support, ASH support, etc.);
- Aircraft identification number and aircraft type; and
- Personal information of the alleged violator or witnesses, which may include:
    - Airman's full name;
    - Airman's telephone number;
    - Airman's mailing address;
    - Airman's certificate number;
    - Company name;
    - Full name of company's authorized representative;
    - Job title;
    - Company's address;
    - Date and Place of Birth;
    - Citizenship; and
    - Sex.

SEIT employees scan all case-related supporting documentation and file them in an encrypted shared drive by case number. Once the supporting documentation is scanned, the SEIT employee conducts a quality control check of the scanned document and then destroys all paper copies.

SEIT employees then conduct interviews to gather additional information about the case and enter information obtained while conducting interviews into an open-text field. The information that is entered into the open-text field may include the names, phone numbers and/or addresses of individuals interviewed, and information associated with the case. Social security numbers (SSN) are not entered in this field. A warning banner is present cautioning users to only enter the minimum and relevant PII necessary to conduct the investigation.

The SEIT employee analyzes all information in iTRAK to determine if there is a safety violation. If there is no safety violation, the SEIT employee enters the determination of no safety violation, the closure date, and then closes the case in iTRAK. Alternatively, if a potential violation exists, the SEIT employee annotates the violation and continues the investigation in iTRAK. The Enforcement Information System (EIS)[4] is used to record all

[4] The PIA for EIS can be found here.

enforcement actions necessary to resolve the safety violation(s), but none of that information is entered into iTRAK.

Analyst Notebook

For each case evaluation, the SEIT employees conduct searches within iTRAK to look for historical information on an aviation entity and/or individual. The Analyst Notebook is used to support modeling and analysis of the information in cases. Analyst Notebook provides a pictorial view of data that reveals relationships between entities, (information such as identification of aircraft flown by an airman, whether the registered owner also has a company under the same name, airmen aircraft ownership, address of airman, aircraft, and company). Analyst Notebook does not collect or store data but receives information from iTRAK that includes the airman's full name, telephone number, mailing address, certificate number, DOB, citizenship, sex, company name, and address, the full name of the company's authorized representative, job title, aircraft identification number and type. Analyst Notebook displays the complainant's information such as name, mailing address, email address, telephone number, subject of complaint and description of the complaint. Analyst Notebook displays that data in a visual format that helps inspectors analyze the data relating to an investigation. It provides a method to support inspectors in their analysis, helping to navigate through the data. Analyst Notebook does have printing and saving capabilities; however, users are informed not to print or save any pictorial views that are displayed.

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

[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

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 informing individuals of the purposes for which the FAA collects, uses, and retains PII in iTRAK during investigations. When SEIT receives safety complaints from other FAA office and federal agencies, the FAA is not collecting information from an individual so notice is not provided but could be provided at the point of collection. SEIT employees enter information into open text fields that is received while conducting interviews. The information that is entered into the open-text field may include names, phone numbers and/or addresses of individuals interviewed. SEIT employees will read the individual a privacy act statement prior to conducting the interview.

The FAA retrieves complaint records in iTRAK by name, and therefore, the information is part of a system of records under the Privacy Act of 1974. The FAA protects and maintains these records in accordance with the following DOT-published SORNs: DOT/FAA 845 *Complaint Intake System*, 87 FR 61649 (October 12, 2022) and DOT/FAA 852 *Complaint Investigations System*, 87 FR 61137 (October 07, 2022). iTRAK also maintains account creation records in accordance with DOT/ALL 13, "*Internet/Intranet Activity and Access Records,*" 67 FR 30758 (May 7, 2002). Lastly, the publication of this PIA further demonstrates DOT's commitment to providing appropriate transparency regarding iTRAK.

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.

iTRAK may receive complaints from individuals by email, postal mail, and referrals from other FAA offices and agencies. SEIT employees enter information into iTRAK open text fields while conducting interviews. The information that is entered into the open-text field iTRAK may include names, phone numbers or addresses of individuals interviewed. Certain records pertaining to investigations are exempted. Under the provisions of the Privacy Act individuals may request searches to determine if any records appear in an FAA system of records. Individuals wishing to know if their records appear in this system may inquire in person or in writing to:

Federal Aviation Administration

Privacy Office
800 Independence Avenue, SW
Washington, DC 20591

The request must include the following information:

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

Individuals should make their request to contest information about themselves in iTRAK in writing, detailing the reasons for why their records should be corrected and addressing their letter to the following address:

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

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.

iTRAK processes information for the purpose of conducting investigations. SEIT receives safety complaints for evaluation by email or letters via U.S. postal mail that include the complainant's name, mailing address, email address, telephone number, subject of complaint and description of the complaint. SEIT conducts interviews and enters additional information about the case into the open-text field that may include name, phone numbers and/or addresses of individuals interviewed and information associated with the case. iTRAK is used by SEIT to conduct analysis as it relates to the evaluation of safety complaints, which may lead to formal investigations of safety violations. The authority to conduct evaluations of safety complaints is 49 USC Chapter 447 Title 49 U.S.C. Section 40113. iTRAK does not share information with other FAA systems.

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.

iTRAK maintains evaluation of safety complaints case files of potential FAA safety violations. iTRAK contains the minimum necessary PII to enable SEIT employees to adequately evaluate and analyze cases assigned to them. SEIT employees are trained in collecting only the minimum necessary information to adequately conduct and analyze safety complaints.

iTRAK maintains records for evaluation case files and iTRAK information access records in accordance with the following National Archives and Records Administration (NARA) schedules:

1. NARA Schedule DAA-0237-2021-0013, *iTRAK System*. This record schedule provides that investigative case file records are temporary and destroyed 30 years after the cutoff at the conclusion of the investigation.

2. NARA General Records Schedule (GRS) 3.1, *General Technology Management Records*, approved November 2019, govern the use of networks and iTRAK. Under this schedule, network usage records are destroyed 3 years after project activity or transaction completion; but may be kept longer if required for business use.

3. NARA General Records Schedule (GRS) 3.2, *Information Systems Security Records*, approved January 2023, govern system access records. Under that schedule, system access records are destroyed when business use ceases.

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.

SEIT employees use iTRAK to support case evaluations of safety complaints and potential violations of FAA statutes and regulations and provide analysis of these investigations. Records in iTRAK are maintained in accordance with DOT/FAA 845, "*Complaint Intake System*", 87 FR 61649, Oct.12, 2022. In addition to other disclosures generally permitted under 5 U.S.C § 552a(b)(3) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DOT as a routine use pursuant to 5 U.S.C. §552a(b)(3) as follows:

1. To the Federal Bureau of Investigation, U.S. Customs Service, and the Department of Defense, the initial SUP complaints received by FAA, for their use in any civil/criminal investigations when an FAA suspected unapproved parts case is initiated.

2. Routine use (2)(a) and (b) apply only to records pertaining to noise complaints, and do not apply to information contained in related hotline or whistleblower protection complaint files. Pursuant to routine use (2), the FAA may disclose:
a. To airport sponsors, federal agencies and departments operating manned and unmanned aircraft outside FAA's regulatory jurisdiction, and other operators of aerial landing and takeoff sites, records relating to noise complaints stemming from their operations to ensure consistency between the FAA and these entities on noise complaints.
b. To man and unmanned aircraft operators when necessary to resolve a complaint pertaining to the operator, or when necessary to ensure consistency between the FAA and the operator in responding to noise complaints. Records disclosed pursuant to this routine use are limited to the following information: geolocation only to the extent necessary to identify the general location of the noise complaint; time and date of complaint; and description of the complaint or inquiry. Complainant names and contact information will not be disclosed pursuant to this routine use; and
3. To officials of labor organizations recognized under 5 U.S.C. chapter 71, access to all information when relevant and necessary to their duties of exclusive representation concerning AVS's Voluntary Safety Reporting Program.
The sharing of safety evaluation information in the iTRAK system is conducted in accordance with DOT/FAA 852 - Complaint Investigations System - 87 FR 61137- October 07, 2022). In addition to other disclosures generally permitted under 5 U.S.C. §552a(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:

1. To the Federal Bureau of Investigation, U.S. Customs Service, and the Department of Defense, the initial SUP complaints received by FAA, for their use in any civil/criminal investigations when an FAA suspected unapproved parts case is initiated.
2. Routine use (2)(a) and (b) apply only to records pertaining to investigations into noise complaints, and do not apply to information contained in files related to other types of investigations described in this notice. Pursuant to routine use (2), the FAA may disclose:

a. To airport sponsors, federal agencies and departments operating manned and unmanned aircraft outside FAA’s regulatory jurisdiction, and other operators of aerial landing and takeoff sites, records relating to noise complaints stemming from their operations to ensure consistency between the FAA and these entities on noise complaints; and

b. To man and unmanned aircraft operators when necessary to resolve a complaint pertaining to the operator, or when necessary to ensure consistency between the FAA and the operator in responding to noise complaints. Records disclosed pursuant to this routine use are limited to the following information: geolocation only to the extent necessary to identify the general location of the noise complaint; time and date of complaint; and summary reports of the complaint or inquiry and related

investigation. Complainant names and contact information will not be disclosed pursuant to this routine use.

3. To officials of labor organizations recognized under 5 U.S.C. chapter 71, access to all information when relevant and necessary to their duties of exclusive representation concerning AVS's Voluntary Safety Reporting Program.

The sharing of user account information in the iTRAK system is conducted in accordance with SORN DOT/ALL 13, "*Internet/Intranet Activity and Access Records*", 67 FR 30758 (May 7, 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:

a. To provide information to any person(s) authorized to assist in an approved investigation of improper access or usage of DOT computer systems.
b. 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.
c. 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.
d. To other government agencies where required by law.

DOT may also disclose iTRAK information outside DOT pursuant to 15 additional routine uses applicable to all DOT Privacy Act systems of records. 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).

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).

For iTRAK, the FAA collects, uses, and retains data that is relevant and necessary for the purpose to collect, store, and conduct analysis as it relates to the evaluation of safety complaints, which may lead to formal investigations of safety violations. The SEIT employee manually enters information into iTRAK. As information is being entered, the SEIT employee conducts a quality check to ensure the information is correct.

All case-related hard files are scanned and filed in an encrypted shared drive by the case number assigned by iTRAK. A quality check of scanned files is performed to ensure that all files are appropriately scanned and readable. Once the documents are scanned, the hard

copies are destroyed. In addition, SEIT employees all have access to Safety Performance Analysis (SPAS) as part of their regular duties and therefore SPAS is available as a tool to confirm the accuracy of the individual's name and contact information.

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.

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 National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations, dated September 2020 (includes updates as of Dec. 10, 2020).

iTRAK employs specific administrative, technical, and physical measures to protect PII against loss, unauthorized access, or disclosure. Personnel receive guidance on their duties related to collecting, using, processing, and securing PII.

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, 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.

In addition to these practices, the FAA will implement additional policies and procedures as they relate to the access, protection, retention, and destruction of PII. Federal employees and contractors who work with iTRAK 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, as well as FAA Order 1370.121B. The FAA will conduct periodic privacy compliance reviews of iTRAK.

Responsible Official

Edward Cardenas
System Owner
Special Emphasis Investigations Team

Prepared by: John Gulisano, Acting FAA Chief Privacy Officer

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN MARIE GORMAN Digitally signed by KARYN MARIE GORMAN Date: 2025.09.10 16:06:23 -04'00'