



U.S. Department of Transportation
Privacy Impact Assessment (PIA)

Federal Aviation Administration (FAA)
Office of Audit & Evaluation (AAE)
FAA Hotline & Whistleblower Information System
(FHWIS)

Responsible Official

Barbara Barnet
barbara.barnet@faa.gov
202 -267-9000

Reviewing Official

Karyn Gorman
Acting Chief Privacy Officer
Office of the Chief Information Officer (OCIO)





Executive Summary

The FAA's Office of Audit and Evaluation (AAE) manages the FAA Hotline & Whistleblower Information System (FHWIS). FHWIS is a web-based application used for tracking voluntary reports and complaints related to unsafe or unauthorized aviation activities that violate FAA regulations, orders, or any other provision of Federal law related to aviation safety, fraud, waste, abuse, misconduct or mismanagement related to FAA programs, personnel, organizations or facilities or safety disclosures made in conjunction with the Wendell H. Ford Aviation and Reform Act for the 21st Century (AIR21). Reports and complaints are accepted for evaluation from FAA employees or contractors, air carrier employees, the aviation community, law enforcement, and members of the public. Anonymous reports are accepted, unless they are filed as an AIR21 disclosure, which require the identity of the person filing the report.

The FAA is publishing this Privacy Impact Assessment (PIA) for FHWIS in accordance with Section 208 of the E-Government Act of 2002 because the system processes personally identifiable information (PII) from members of the public including air carrier employees, the aviation community, and law enforcement.

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

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

¹Office 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).



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 Audit and Evaluation (AAE) manages the Federal Aviation Administration (FAA) Hotline & Whistleblower Information System (FHWIS). FHWIS replaces and consolidates the functions of two formerly separate systems, the FAA Hotline Information System (FHIS) and FAA's Whistleblower Protection Program (WBPP).

The FHIS was deployed in February 2017 to provide a more efficient and centralized data system for the recording and tracking of Safety and Administrator hotlines complaints. FHIS was a web-based application used for tracking voluntary reports and complaints related to unsafe or unauthorized aviation activities that violate FAA regulations or other authorities related to aviation safety, waste, fraud, or other misconduct or mismanagement regarding FAA programs, personnel, organizations, or facilities.

The FAA's Whistleblower Protection Program (WBPP) was established as a result of the Wendell H. Ford Aviation and Reform Act for the 21st Century (AIR21) as well as the passage of the FAA Modernization and Reform Act of 2012, which outlines WBPP responsibilities. WBPP tracks complaints and reports of alleged aviation safety concerns from employees of U.S. air carriers, air carrier contractors, and air carrier sub-contractors.

FHWIS is a cloud-based application used by AAE that supports the FAA's mission to promote safety and regulate civil aviation as defined in 49 U.S.C § 106(t), FAA Order 1100.167B ("The Office of Audit and Evaluation"), FAA Order 1070.1, ("FAA Hotline Program"), and the Wendell H. Ford Aviation and Reform Act for the 21st Century (AIR21).



There are two ways to interface with FHWIS: 1) access for those users who need to assign, manage, or review case reports or maintain the system, and 2) a public-facing functionality allowing submission of a complaint using the FHWIS web form. Access to FHWIS is limited to FAA employees and contractors (system administrators and those that manage the system/program) with a need-to-know and who have been identified by AAE as requiring access to the system or a specific group to which they are assigned. FHWIS is accessed through Uniform Resource Locator (URL) <https://fhwis.faa.gov/>. Users access the system using their Personal Identity Verification (PIV) card and authentication is performed using MyAccess.² All users must first be authorized by a system administrator. FHWIS provides additional security for the data by encrypting data fields at rest within its database.

Submitting a Complaint in FHWIS:

The investigation process begins when an individual submits a complaint. Complaints may be submitted by electronic web form submission or by mail.

Submitting a Hotline or AIR21 Whistleblower Complaint via web form

The complainant initiates a complaint by navigating to one of the electronic web forms at:

- FAA Hotline: <https://hotline.faa.gov/>
- AIR21 Whistleblower: <https://wbpp.faa.gov>

Though the complainants do not need to authenticate to the website, they must acknowledge a pop-up Privacy Act Statement (PAS) before accessing the FHWIS web forms. The FAA electronic web forms specifically advise complainants not to include their date of birth and Social Security Number (SSN) and does not have designated fields for either. The submission is completed by the complainant who enters data into mandatory and optional fields in the appropriate web form.

FAA Hotline web forms (Required fields):

1. Reporter Type (The user is required to indicate whether they are a(n)):

- Aviation Industry Member
- Passenger or Traveler
- FAA Employee
- FAA Employee Filing on Behalf of Someone Else

²MyAccess provides 80,000 employees and contractors of the DOT and FAA the capability to log into an application using their personal identity verification (PIV) card, thereby reducing the number of passwords an employee would be required to create, use, and recall for various applications.



- FAA Contractor
 - Organizational Designation Authorization (ODA) Administrator/Unit Member (Current/Former)
 - Law Enforcement Member
 - Attorney, Law Firm or Aviation Organization
 - Member of Aviation Community
 - General Public Member
2. Confidentiality (Complainants are required to select a level of confidentiality of their submission):
- Confidential – Complainant consents to the disclosure of their identity to FAA personnel for the purpose of conducting an assessment, inquiry or investigation; other FAA personnel with a need to know for official FAA business purposes; or pursuant to routine uses as described in the Hotline System of Records Notification ([DOT/FAA 845, Administrators Correspondence Control and Hotline Information System, ACCIS, Administrator’s Hotline Information System, AHIS and Consumer Hotline Information System, CHIS, 65 FR 19526 \(April 11, 2000\)](#)).
 - Office of Audit and Evaluation (AAE) Only – Complainant consents to the disclosure of their identity to AAE personnel only. If assessment, inquiry or investigation of the matter is referred to an office outside of AAE, the complainants contact information will not be provided to that office. (Note: Disclosure may be required under the provisions in 14 U.S.C. § 106(t)(3)(B), as noted above.)
 - Anonymous – The complainant requests to remain anonymous. Contact information will not be collected as part of their report. This selection may severely limit the FAA’s ability to address the submission.

If the complainant selects confidential, or AAE Only, the only contact information collected is their name and email address. Complainants who select Anonymous will not be permitted to enter their contact information. In those instances, the only information that is collected on complainants is their “Reporter Type.”

3. Contact Information (requested of the complainant):
- First Name
 - Last Name
 - Email
4. Narrative: Description of the complaint, which may include names of individuals who may have knowledge of the complaint. This is an open text field where the complainants are advised not to include personal data such as birthdates or SSN.



5. Other Reports on the Same Subject Matter: In this section, the complainants indicate whether they know of any other related complaints pertaining to the same issue that have been made in a different (or same) forum and to identify any other division of FAA, or external federal or state agency to which the issue was reported.

FAA Hotline web forms (Optional Fields):

1. Contact Information of complainant:

- Contact Phone
- Company
- Position
- Street Address
- City
- Country
- State
- Zip Code

2. What the complainant is reporting (If Applicable):

The complainant is asked to select whether their report is related to either a possible violation of an FAA regulation, order or any other provision of Federal Law related to aviation safety or of the National Airspace System, or suspected fraud, waste, abuse or misconduct related to FAA programs, personnel or facilities. The data collected may include:

- Event Date and Time
- Event Location (City and State)
- Airline or Aviation Company
- Flight Number
- Departure Location
- Arrival Location
- Aircraft Registration

Who the complainant is reporting (If Applicable)

- First Name
- Last Name
- Email
- Phone
- FAA Contact Company (if applicable)
- Title
- Web Address



3. File Upload (attachments)

Submitting a Whistleblower Complaint (AIR21) using an electronic web form:

For a complaint to be accepted under the WBPP, complainants must:

- Be or have been an employee of a U.S. air carrier or a contractor or subcontractor of a U.S. air carrier (disclosures from aviation manufacturing entities are also accepted)
- Have reported a potential air carrier safety violation to their company and/or the FAA, and
- Believe they are being or have been discriminated against by their employer for making that report.

AIR21 Whistleblower web form (Required Fields):

1. Contact Information:

- First Name
- Last Name
- Email
- Company Name

2. Type of entity (select one):

- Air Carrier
- Air Carrier Contractor
- Air Carrier Sub-contractor
- None of the Above

3. Job of complainant (select one):

- Pilot
- Cabin Crew
- Dispatcher/Flight Follower
- Mechanic
- Gate/Station Agent
- Ground Crew
- Manufacturing
- Other

4. Date the complainant learned of the job discrimination (select date)

5. Type of discrimination (select one):

- Discharge



- Suspension
 - Transfer
 - Intimidation
 - Change in schedule/location
 - Other
6. Whether the complainant has submitted an AIR21 Discrimination claim with OSHA on the matter
7. For safety Complaints, a description of the complaint. Here complainants are asked to provide details below of the air carrier safety violation(s) that they are reporting. Complainants are asked to include dates/aircraft numbers/part types and numbers/airport information/witnesses as appropriate.

Optional Fields: AIR21 Whistleblower web form.

- Street Address
- City
- State (select one)
- Zip Code
- US Territory or Country if outside of US (select one)
- Contact Phone
- Type of company:
 - Scheduled Airline
 - Charter or On-Demand
 - Repair Station
 - Training Center
 - Aircraft of Parts Manufacture
 - Other
- Company's FAA certificate number
- Company Phone
- Company street address the complainant works at
- Company City
- Company State (select one)
- Company Zip
- Date the potential violation was reported to the company or FAA (date picker)
- If reported to FAA, to whom or what office.

The WBPP does not accept anonymous complaints. If an individual makes an anonymous complaint, their complaint will be transferred to the FAA Hotline.



Once the complainant completes and submits an FHWIS web form, the data from the form is routed through a secure firewall and is automatically transferred into FHWIS. The complainant receives a pop-up box confirming receipt of their report along with a request number and the hotline email address. This provides the complainant the ability to send additional information or attachments to the FAA.

Submitting a complaint by Mail

A complaint may be mailed to:

Federal Aviation Administration
Office of Audit and Evaluation
Attn: AAE, Office of Whistleblower and Aviation Safety Investigations
800 Independence Ave SW
Washington, DC 20591

Information from mailed correspondence will be entered into FHWIS manually and the hard copies will be scanned and uploaded into the system. Once the electronic copy is verified as accurate and complete, all hardcopies of the correspondence will be destroyed. Information included in the mailed copy may contain the complainants name, contact information, and pertinent information about the complaint and/or the alleged violator.

Processing a Report/Complaint in FHWIS:

FAA Hotline

Each complaint is evaluated to determine appropriate action based on the subject matter of the complaint. Various factors are considered to include whether there is sufficient information to investigate, previous reporting, or if the FAA is the proper authority over the subject matter. The complainant receives an automatic acknowledgement of receipt of the complaint with the case number. If additional information is needed to complete an evaluation, AAE may contact the complainant to follow-up and/or request additional information. AAE may correspond with the complainant using the FHWIS system email or by phone (if provided).

If the hotline complaint is accepted for further action, the hotline is referred through FHWIS to the appropriate office with instructions, such as to investigate and report on the allegations, or other appropriate action. The assigned office is notified via email, which includes a password-protected copy of the complaint. When appropriate, the complainant is notified that the hotline complaint has been referred to another office.



If no further action by AAE is warranted, the matter is closed out in FHWIS. If appropriate, an email is sent to the reporting individual regarding the status.

Complaints accepted by other forums (e.g., ASH, Appeals Board, Equal Employment Office, Bargaining Unit, Office of Inspector General, civil or criminal litigation, etc.) will be closed out in the FHWIS upon notification of acceptance or confirmation that the subjects of the complaint are already being addressed through another venue. If the reporting individual provides contact information, she or he will be notified that the matter is being handled by another venue outside the Hotline process.

AIR21

All valid AIR21 Whistleblower cases are converted into a password protected Portable Document Format (pdf) and provided to the Department of Labor's Occupational Safety and Health Administration (OSHA) in accordance with the December 1, 2015, Memorandum of Understanding (MOU) between OSHA and the FAA. The FAA will also provide OSHA, via email, with the general results of any AIR21 investigation conducted by the FAA. Such notification will only include the complainant's name, case number, OSHA number (if extant), and whether there was a violation of a regulation, order or standard relating to air carrier safety.

Investigating an FAA Hotline or AIR21 Complaint:

When an investigation is warranted, FAA investigative offices handle the investigative process outside of the FHWIS. Their investigative records reside with the investigative office, not in FHWIS, and are not considered part of the complainant's file. Once the investigation is completed, the investigative office provides an electronic copy of either the Investigative Results Report (IRR) for FAA Hotlines or a Report of Investigation (ROI) for AIR21. The IRR details a summary of the allegations, the case number, the investigative findings, as well as any corrective action, if applicable. It may also include some or all of the PII included in the original complaint, such as the subject or violator name, witnesses interviewed, and complainant's name and contact information. AAE conducts a sufficiency review of each IRR or ROI. If deemed sufficient, the hotline case is closed. An AIR21 case will not be closed until the ROI is deemed sufficient and all corrective actions are adequately completed. When appropriate, the complainant (if known) may receive an email from AAE that provides the general findings. AAE does not provide any investigative details or PII to the complainant.

Reconsideration of Investigative Findings:



FAA Hotline

The complainant may request reconsideration of the investigative findings if they identify or provide information that was not considered during the initial investigation that may have changed the outcome of the investigation. The complainant may submit a written request for reconsideration of their report to AAE. Requests for reconsideration must include the specific allegations that were not addressed in the original response, the complaint reference number, and the reason(s) why the complainant believes that their allegations were not addressed to include evidence to support their claim. AAE evaluates requests for reconsideration to determine if further action is warranted. If accepted, the matter will be re-actioned to the original investigating office under the same complaint reference number for response to the issues outlined in the reconsideration request. Confidential complainants may maintain confidentiality during the reconsideration process.

AIR21

There is no formal reconsideration process for AIR21 Whistleblower investigations. Prior to reviewing a request for reconsideration, the submitter will be required to obtain a copy of the ROI through a request under the Freedom of Information Act (FOIA). In the rare occasion that a submitter has a valid safety concern, the WBPP staff determines any required next steps to include re-investigation, a possible new AIR21 case for investigation, or whether to deny the appeal request.

FHWIS users can generate FHWIS system reports for management, special data requests, FOIA response, or other purposes. System reports that could be generated include reports on various statistics or other information, such as number of cases assigned to a specific investigative branch or an investigator. Any of the PII present in FHWIS could be included in these reports.

PII is collected from the person who submits the report to FHWIS for AAE to properly open and manage investigations. Further, PII is required by OSHA to investigate allegations of discrimination.

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) v3³, 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 Organizations⁴.

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 ensure individuals are aware of the FHWIS and the purposes for which the FAA collects and maintains PII in support of the FHWIS. The FAA Hotline and AIR21 complaint processes are well known throughout the aviation industry. FAA also notifies the public of the FHWIS through FAA's public website available [here](#).

The FHWIS Electronic Web Forms display a Privacy Act Statement (PAS) that informs complainants of their rights afforded under the Privacy Act and applicable laws and regulations. As required, the PAS discusses the Department's privacy practices regarding the collection, use, sharing, maintenance, and disposal of PII. If any changes to law or policy occur which require modification of the PAS, it will be modified accordingly.

Additionally, all substantive FHWIS records are maintained in accordance with the following Department's System of Records Notices (SORNs):

- [DOT/FAA 845, Administrators Correspondence Control and Hotline Information System, ACCIS, Administrator's Hotline Information System, AHIS and Consumer Hotline Information System, CHIS, 65 FR 19526 \(April 11, 2000\)](#), and
- [DOT/FAA 852, Suspected Unapproved Parts \(SUP\) Program, 65 FR 83124 \(December 29, 2000\)](#).⁵

³ <http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf>

⁴ http://csrc.nist.gov/publications/drafts/800-53-Appendix-J/IPDraft_800-53-privacy-appendix-J.pdf

⁵ The FAA is currently updating SORNs 845 and 852. All investigative records in FHWIS are a part of SORN 852 and only the intake records will be part of SORN 845.



In addition, [DOT/ALL 13, *Internet/Intranet Activity and Access Records*, 67 FR 30757 \(May 7, 2002\)](#) covers login credentials, audit trails, and security monitoring for FAA employees and contractors who are part of the FHWIS program and/or manage the system.

Finally, the publication of this PIA demonstrates DOT's commitment to provide appropriate transparency into the FHWIS.

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.

Complainants may voluntarily submit PII through the electronic complaint form or via mail. If utilizing a web form for submission, the complainant can review and make changes to the information before submitting. However, once that information is submitted, the complainant cannot directly change the FHWIS information because it has been migrated to the application itself, which is only accessible to FAA employees with system access.

Updates or corrections to information stored in FHWIS can be made by reporting through the FHWIS Web Form (<https://hotline.faa.gov/>, <https://wbpp.faa.gov/>). If verified, an authorized hotline analyst could make such changes in FHWIS and note the reasons for the change.

In addition, complainants may request a search to determine if records about them are maintained in an FAA Privacy Act system of records. To request a search, individuals may inquire in writing by sending a request to:

Federal Aviation Administration
Office of Audit and Evaluation (AAE)
800 Independence Avenue, S.W. Washington, D.C. 20591
Attn: AAE, Room 911

The request must include:

- The individual requestor's name
- Mailing address



- Phone number or email address
- A description of the records sought, and if possible, the location of the records and system(s) acronym(s).

Complainants seeking a correction of records pertaining to them that are stored in FHWIS must make their requests in writing. Requests must detail the correction and the reasons the records should be so corrected. Requests for corrections of records may be sent to:

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

Or Privacy@faa.gov

Individuals may also use the above address to register a complaint or question regarding FAA's privacy practices.

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.

FHWIS is authorized under:

- Title 49 United States Code (USC), Section 106(t), Office of Whistleblower Protection and Aviation Safety Investigations.
- The Wendell H. Ford Aviation and Reform Act for the 21st Century (AIR21), Section 519, Chapter 42121 which requires a complainant under AIR21 to provide sufficient information to include personal identity, for an investigation to be feasible.

As discussed in the overview, FHWIS records are used to document and process allegations of violations of any order, regulation, or standard of the FAA or any other Federal law relating to air carrier safety; to document and process allegations of fraud, waste, abuse, or misconduct related to FAA programs, personnel, organizations, or facilities related to FAA programs or personnel; and to monitor and track case assignments, disposition, status, and investigative results, and create and report statistical information.



The FAA does not use the PII for any other purposes.

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.

The FAA collects the minimum amount of PII and other information necessary to analyze and process complaints. For the FAA Hotline, the system allows the complainant to choose to remain anonymous. If they choose not to remain anonymous, the only mandatory fields collecting PII are the complainants first and last name and email address. The complainant voluntarily provides all other information to the system if they feel that the information is related to the complaint.

The FHWIS web form informs the complainant “DO NOT include any personal data such as birthdate or Social Security Number (SSN)” in the narrative (open text) field.

Records in FHWIS are maintained in accordance with the following National Archives and Records Administration (NARA) Schedules:

The FAA Hotline Information System (FHIS) Records and Whistleblower Protection Program (WBPP) Records maintained in FHWIS are covered under the [FAA Hotline Tips, complaints and Reporting Systems schedule, published August 17, 2020](#), under which the records are temporary and should be cut off after case is closed and destroyed 3 year(s) after cut off, under DAA-0237-2019-0012.

FHWIS paper and electronic files and records will be destroyed 3 years after case closure in accordance with DAA-0237-2019-0012, except for Suspected Unapproved Parts (SUPS) records, which are covered under [DAA-0237-2019-0010](#) and are have a cut-off at the end of the calendar year in which cases are closed and will be destroyed 8 years after cut-off.

In addition, authentication and access records are covered under [NARA General Records Schedules \(GRS\) 3.2 Information Systems Security Records, September 2016, Item 030](#), are temporary and should be destroyed when business use ceases, under DAA-GRS-2013-0006-0003.

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.

FAA employs multiple controls to promote use limitation and reduce the risk of information maintained in FHWIS from being used for extraneous purposes. Access to FHWIS is limited to AAE personnel or other FAA employees with a need-to-know. Access to the system is reviewed and approved by AAE management. Further, when a pdf is created, AAE includes a coversheet with the pdf that details guidance about the proper handling of that record.

FAA limits sharing of Privacy Act records collected, used, and maintained as part of FHWIS in accordance with the applicable SORNs:

- [DOT/FAA 845, Administrators Correspondence Control and Hotline Information System, ACCIS, Administrator's Hotline Information System, AHIS and Consumer Hotline Information System, CHIS, 65 FR 19526 \(April 11, 2000\), and](#)
- [DOT/FAA 852, Suspected Unapproved Parts \(SUP\) Program, 65 FR 83124 \(December 29, 2000\).](#)⁶

Note: Under DOT/FAA 852, *Suspected Unapproved Parts*, 65 FR 83124 (December 29, 2000), this system of records is exempted from certain provisions of The Privacy Act. The purpose of the exemptions is to protect investigatory materials compiled for non-criminal law enforcement purposes. The exemptions claimed for this system are pursuant to 5 U.S.C. 552a(k)(2).

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 this system may be disclosed outside of DOT as a routine use pursuant to 5 U.S.C. § 552a(b)(3) as follows:

- Referral to the appropriate action office within or outside the Department or agency for preparation of a response.

⁶ The FAA is currently updating SORNs 845 and 852. All investigative records in FHWIS are a part of SORN 852 and only the intake records will be part of SORN 845.



- Referral to the appropriate agency for actions involving matters or law, of regulations beyond the responsibility of the agency or Department, such as the Department of Justice in matters of law enforcement.
- As a data source for management information, such as briefing material on hearings, trend analysis, responsiveness.

Further, the Department has published 14 additional routine uses applicable to all DOT Privacy Act SORNs, including this system. The routine uses are published in the Federal Register at [75 FR 82132, December 29, 2010](#) and [77 FR 42796, July 20, 2012](#).

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 FAA employs a combination of processes to ensure the quality and integrity of FHWIS data. FHWIS receives complaint information directly from the complainants. To ensure data completeness, analysts review the input data to ensure all required data needed to initiate a complaint is obtained. If information is incomplete and follow-up is required, the analyst can contact the complainant for more complete information. If the complainant believes the FHWIS contains inaccurate information, the complainant may contact the AAE office using the provided email or mailing address identified above. Additionally, the investigative process helps verify the accuracy and integrity of a complaint.

In addition, alleged subjects of the complaint cannot make corrections to any of their information within the system that was a part of the original complaint. The alleged subjects can only provide details and updated information as a part of an investigation if one is initiated.

Lastly, FHWIS logs are audited as needed. The audit logs that are generated from the audits are reviewed by business owner to assure proper use of the system. These activities and audit records are time stamped.

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. 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, 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.

Access to the system is limited with those with a “need to know” and access is approved by a system administrator. FHWIS employs appropriate safeguards to protect PII against loss or unauthorized access, destruction, usage, modification, or disclosure using controls including systems access controls, encryption, role-based access to information within FHWIS, and appropriate training, supervision, and system management.

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.

FHWIS follows directives in 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 policy, 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 implements additional policies and procedures as they relate to the access, protection, retention, and destruction of PII. Federal employees and contractors who work with FHWIS 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 U.S. Department of Transportation 1370.121B. The FAA will conduct periodic privacy compliance reviews of FHWIS, as related to the requirements of OMB Circular A-130, Managing Information as a Strategic Resource.



Responsible Official

Barbara Barnet
Business Owner

Supervisory Investigator, Office of Audit and Evaluation (AAE)

Prepared by: Barbara Stance, FAA Chief Privacy Officer

Approval and Signature

Karyn Gorman
Acting Chief Privacy Officer
Office of the Chief Information Officer (OCIO)

DOT Privacy Office - Approved - 09 19 2022