



U.S. Department of Transportation
Privacy Impact Assessment

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

Responsible Official

Anthony Wheat
Email: anthony.w.wheat@faa.gov
Phone Number: 813-500-8744

Reviewing Official

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





Executive Summary

The FAA's Office of Audit and Evaluation (AAE) along with the Office of Flight Standards (AFX) manages the Federal Aviation Administration (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 whistleblower safety, retaliation, or other related disclosures. FHWIS operates under the authority of [Title 49 United States Code \(U.S.C.\), Section 106\(t\)](#), *Office of Whistleblower Protection and Aviation Safety Investigations; FAA Modernization and Reform Act of 2012* § 341(3)(A), Pub. L. No. 112-95, 126 Stat. 78; 44 U.S.C. § 3101; and *The Wendell H. Ford Aviation and Reform Act for the 21st Century* (AIR21), Section 519, Chapter 42121.

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 attorneys, law firms or aviation organizations, aviation industry members, FAA contractors FAA employees filing on behalf of someone else, general public members, law enforcement members, Organizational Designation Authorization (ODA) administrator/unit members (current/former), and passengers or travelers.

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

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).



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

AAE along with AFX manages the FAA FHWIS. FHWIS replaced and consolidated the functions of two formerly separate systems, the FAA Hotline Information System (FHIS) and FAA's Whistleblower Protection Program (WBPP). The FHWIS case module was deployed into production in August of 2022 and the investigation module was released into production on November 1, 2022. The Whistleblower Ombudsman webpage was introduced on March 27, 2023. FHWIS operates under the authority of [Title 49 U.S.C., Section 106\(t\)](#), *Office of Whistleblower Protection and Aviation Safety Investigations; FAA Modernization and Reform Act of 2012* § 341(3)(A), Pub. L. No. 112-95, 126 Stat. 78; 44 U.S.C. § 3101; and *The Wendell H. Ford Aviation and Reform Act for the 21st Century (AIR21)*, Section 519, Chapter 42121.

The Office of Foundational Business, Safety Risk Management Division (AFB-400), investigates safety hotlines and whistleblower complaints assigned from AAE. FAA aviation safety investigators conduct investigations in accordance with FAA regulatory guidance. AFB-400 also oversees the Flight Standards field offices, which investigate safety hotlines within the realm of their office oversight responsibilities.

FHWIS is a cloud-based application used by AAE and AFX that supports the FAA's mission to promote safety and regulate civil aviation.

There are two ways to interface with FHWIS: 1) access for those internal FAA 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 page. 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 and AFX as requiring access to the system or a specific group to which they are assigned. FHWIS is accessed through an internal FAA, non-publicly available Uniform Resource Locator (URL) [Home](#). 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 the system administrator. FHWIS provides additional security for the data by encrypting data fields in transit and at rest.

Submitting a Complaint in FHWIS:

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

Submitting a Hotline or AIR21 Whistleblower Complaint via web page at URLs:

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

- FAA Hotline: [Home](#)
- 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 pages. The FAA electronic web pages specifically advise complainants: Do NOT include Date of Birth (DOB) and Social Security Number (SSN). Additionally, FHWIS does not have designated fields for either DOB or SSN. The submission is completed by the complainant who enters data into mandatory and optional fields in the appropriate web page.

FAA Hotline Web Pages (Required fields):

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

- Attorney, Law Firm Member
- Aviation Industry/Organization Member
- FAA Contractor
- FAA Employee
- FAA Employee Filing on Behalf of Someone Else
- General Public Member
- Law Enforcement Member

² MyAccess 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.



- Organizational Designation Authorization (ODA) Administrator/Unit Member (Current/Former)
- Passenger or Traveler

2. Confidentiality (Complainants are required to select a level of confidentiality of their submission):

- Confidential – complainant/reporting party consents to the disclosure of their identity to FAA personnel for the purpose of conducting an assessment, inquiry, or investigation; to other FAA personnel with a need to know for official FAA business purposes; or pursuant to routine uses as described in the System of Records Notice (SORN) [DOT/FAA 845, Complaint Intake System](#).
- 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):

- Name (First and Last)
- 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 pages (Optional Fields):



1. Contact Information of complainant:

- 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 Name
- Flight Number
- Departure Location
- Arrival Location
- Aircraft Registration Number

Who the complainant is reporting (If Applicable):

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

3. File Upload (attachment)

Submitting a Whistleblower Complaint (AIR21):

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 or U.S. aircraft/component manufacturer



- 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 page (Required Fields):

1. Contact Information:

- 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. Have you submitted an AIR21 Discrimination claim with Department of Labor Occupational Safety and Health Administration (OSHA) on this matter?

- Yes – If selected enter your OSHA Case Number



- No

7. Safety Complaint – A description of the complaint, provide details below of the air carrier safety violation(s) you are reporting. Include dates/aircraft numbers/part types and numbers/airport information/witnesses as appropriate.

Whistleblower (AIR 21) Web Forms (Optional Fields):

- 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 page (Hotline or Whistleblower (AIR21)), 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 case number.

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, Room 911
Washington, DC 20591

Information from mailed correspondence is entered into FHWIS manually and hard copies 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 violation/violator.

Processing a Report/Complaint in FHWIS:

FAA Hotline

Each complaint is evaluated to determine the 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. For assignments other than AFX, 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.

Internal and external FAA Hotline and Whistleblower complaints are assigned to AFX from within FHWIS.

- Internal Hotline and Whistleblower complaints are reviewed and investigated within the FHWIS, and all documentation and information associated with the investigative records are stored within FHWIS.



- Internal Hotline complaints assigned as a management inquiry or to a headquarters program office are managed and/or investigated outside of FHWIS. The assigned office is notified via email of the assignment by an AFX Hotline POC. The assigned office is provided a password-protected copy of the complaint.
- External Hotline Complaints are managed and/or investigated by AFX field offices outside of FHWIS. The assigned office is notified via email of the assignment. The assigned office is provided a password-protected copy of the complaint, by an AFX Hotline Principal POC.

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.) are 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, they are notified that the matter is being handled by another venue outside the Hotline process.

AIR21

All accepted Whistleblower (AIR21) 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 also provides OSHA, via email, with the general results of any AIR21 investigation conducted by the FAA. Such notification only includes the complainants name, FHWIS case number, OSHA number (if it exists), and whether there was a violation of a regulation, order or standard relating to air carrier safety.

Investigating an FAA Hotline or AIR21 Complaint:

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 FHWIS case number, the investigative findings, as well as any corrective action, if applicable. It may also include some or all the PII included in the original complaint, such as the subject or violator name, witnesses interviewed, and the complainants 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 cannot 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-acted 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 responses, 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.

Submitting a Whistleblower Ombudsman Complaint



The Whistleblower Ombudsman webpage includes a Privacy Act Statement (PAS), and information submitted is sent to the Whistleblower Help mailbox.

1. Complainant/Reporting Party – Required fields:

- Name
- Line of Business (LOB)/ Staff Office (SO)
- Email Address

Whistleblower Ombudsman Web Page (Optional fields):

1. Complainant/Reporting Party – Optional fields

- Phone
- Narrative dialog box

The complainant/reporting party then navigates down and click on the “submit” button. The web page content will be emailed to the Whistleblower Help mailbox.

Submitting a complaint by email:

- 9-AAE-Whistleblower-Help@faa.gov

Submitting a complaint by Mail

A complaint may be mailed to the Federal Aviation Administration, Office of Audit and Evaluation, Attn: AAE, Office of Whistleblower Ombudsman, 800 Independence Ave SW. Room 911, Washington, DC 20591. Information from email and mailed correspondence is stored in an encrypted database outside of the FHWIS system. Hardcopies are scanned and uploaded into a secure Ombudsman folder on the FAA network and destroyed upon verification of a complete electronic copy. Information included in the email and mailed copy may contain the complainant/reporting party name, contact information, and pertinent information about the complaint and/or the alleged retaliator.³

Managing a Whistleblower Ombudsman Complaint

Each complaint is evaluated to determine appropriate action based on the information provided in the complaint, part of this evaluation includes whether this complaint is under the purview of the Ombudsman’s office. If the matter is under the purview of the

³ The FAA employee, FAA contractor, or non-FAA employee or contractor that the complainant/reporting party is filing the complaint about.



Ombudsman's office, the Ombudsman's office will contact the complainant/reporting party for further review.

Whistleblower Ombudsman

If the complaint is accepted for further action, the Whistleblower Ombudsman office interviews the complainant and makes a determination as to whether there is sufficient information to infer that whistleblower retaliation may have taken place. If the Ombudsman's office determines there is a probability that whistleblower retaliation has occurred, the complaint is referred to the appropriate office. If the complaint is not referred, the Ombudsman office advises the complainant/reporting party of other available rights and remedies including that they may contact the Office of Special Counsel.

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 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.

FHWIS is a privacy-sensitive system because it maintains collects, uses, disseminates, and retains PII from (FAA employees or contractors), air carrier employees, the aviation community, law enforcement, and members of the public for the processing of Hotline and Whistleblower (AIR21) complaints. Policies, procedures and practices for

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



information storage, data use, access, notification, retention, and disposal are described herein this PIA.

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 at [FAA Hotline | Federal Aviation Administration](#).

The FHWIS and Whistleblower Ombudsman Electronic Webpages 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.

The FAA protects records subject to the Privacy Act in accordance with the following Department's Published System of Records Notices (SORNs):

[DOT/FAA 845, *Complaint Intake System* 87 FR 61655 \(October 10, 2022\)](#), covers (Hotline and Administrators Hotline records) about air carrier employees, the aviation community, law enforcement, and members of the public that are used for the processing of complaints. The records may include the following PII about (air carrier employees, the aviation community, law enforcement, and members of the public): names, email, addresses.

[DOT/ALL 13, *Internet/Intranet Activity and Access Records* 67 FR \(May 7, 2002\)](#) covers (electronic records (login credentials, audit trails, and security monitoring for FAA employees and contractors) about All DOT employees, contractors, or other users authorized or unauthorized who access the Internet/Intranet through any of the authorized DOT network computers or mainframe/enterprise servers, including individuals who send and receive electronic communications, access Internet/Intranet sites, or access system databases, files, or applications from DOT computers or sending electronic communications to DOT computers) the logs of Internet/Intranet access and use from a DOT computer generally do not directly contain names or similar personal identifiers.

[DOT/FAA 852, *Complaint Investigations System* 87 FR 61649 \(October 12, 2022\)](#) covers records of investigations, findings and resolution of complaints, and reports of unsafe or unauthorized aviation activities concerning the perceived or actual violations of FAA regulation, order, or other provision of Federal law related to aviation safety or practices, including whistleblower and noise complaints. Records maintained in this system include files specific to reports of alleged violations, investigatory materials, investigation results,



individuals' roles in investigations and information on any enforcement actions, alert or notification actions. Individuals (complainants, such as members of the public, FAA employees and contractors, and other individuals alleged to have been involved in the reported alleged violations or other aviation safety concerns) records may include names of complainants, contact information (phone number, address, email address), geolocation of noise, aircraft registration number, airman/mechanic/air carrier certificate number, aircraft tail number, and report/case tracking number (to include, but not limited to, reference number, case number, record number, and control number).

The records may also include the following PII about air carriers, repair stations, mechanics, manufacturers, suppliers, brokers, or individuals who are otherwise directly or indirectly involved in suspected unapproved parts investigations including name and address, phone numbers, and certificate numbers of companies or individuals, their role in Suspected Unapproved Parts (SUP) investigations, information referencing enforcement actions, alert or notification actions, and investigation results.

The publication of this PIA demonstrates DOT's commitment to providing appropriate transparency into the FHWIS 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 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 webpage or via mail. If utilizing the webpage 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 at URLs [Home](#), and <https://wbpp.faa.gov>. If verified, an authorized hotline analyst could make such changes in FHWIS and note the reasons for the change.

Under the provisions of the Privacy Act, individuals may request searches of the FHWIS system to determine if any records have been added that may pertain to them and if such records are accurate. 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).

For all inquiries related to the information contained in the FHWIS, the individual may appear in person, send a request via email (privacy@faa.gov), or in writing to:

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
- A signed attestation of identity

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 has authorized the FAA Administrator to develop systems and/or tools to support business needs by collecting complaints related to aviation safety and/or Whistleblower (AIR21). FHWIS addresses the unique demands of the FAA's workforce and operates under the authority of:



- [Title 49 United States Code \(USC\), Section 106\(t\)](#), Office of Whistleblower Protection and Aviation Safety Investigations. FAA Modernization and Reform Act of 2012 § 341(3)(A), Pub. L. No. 112-95, 126 Stat. 78; 44 U.S.C. § 3101.
- *The Wendell H. Ford Aviation and Reform Act for the 21st Century (AIR21)*, Section 519, Chapter 42121.

FHWIS maintains the following PII on federal employees and contractors for MyAccess. FHWIS receives the end users (FAA employees and contractors) federated ID from MyAccess using the Hypertext Transfer Protocol Secure (HTTPS) for authentication to the system. The PII Sharing Agreement between AFN-AIT MyAccess and FHWIS covers the data exchange.

The FAA uses this access information for purposes of creating and validating login credentials, audit trails, and security monitoring for FAA employees and contractors who are part of the PRISM program and/or manage the system. This use is consistent with the description in the “purpose” section in the SORN [DOT/ALL 13, Internet/Intranet Activity and Access Records 67 FR 30757 \(May 7, 2002\)](#).

FHWIS uses this information in accordance with the purposes for which it is collected: 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.. This information is used in accordance with the description in the “Purpose” section of the applicable SORNs:

- [DOT/FAA 845, Complaint Intake System 87 FR 61655 \(October 10, 2022\)](#)
- [DOT/FAA 852, Complaint Investigations System 87 FR 61649 \(October 12, 2022\)](#)

The PII in the FHWIS system is not routinely used 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 to “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 [FAA Hotline Tips, Complaints, and the AIR21 Whistleblower Protection Program](#) under DAA-0237-2022-0010.

- FAA Hotline and AIR21 Whistleblower Protection Program records are temporary and should be cut off after case is closed. Destroy 3 year(s) after cutoff.

In addition, authentication and access records are covered under [National Archives and Records Administration \(NARA\) General Records Schedule⁵ \(GRS\) 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 and AFX management. Further, when a pdf is created, AAE includes a coversheet with the pdf that details guidance about the proper handling of that record. The PII in FHWIS is used to process Hotline and Whistleblower complaints to FAA employees or contractors, air carrier employees, the aviation community, law enforcement, and members of the public. The FAA does not use the PII for any other purpose.

The FAA/DOT limits the scope of PII collected in FHWIS to support the purpose specified in the following SORNs:

⁵ General retention schedules are used by the FAA to determine how long to maintain an individual’s records and/or when to delete the individual’s records and to promote consistent retention practices.



[DOT/FAA 845, *Complaint Intake System*, 87 FR 61655 \(October 10, 2022\)](#). DOT may disclose records from this system, as a routine use, to an agency, organization, or individual for the purpose of performing audit or oversight operations related to this system of records, but only such records as are necessary and relevant to the audit or oversight activity.

[DOT/FAA 852, *Complaint Investigations System* 87 FR 61649 \(October 12, 2022\)](#) covers the FAA will routinely provide relevant information to the Federal Bureau of Investigation, U.S. Customs Service, and Defense Criminal Investigative Services for their use in any civil/criminal investigations when a SUP case is initiated.

Note: Under [DOT/FAA 852, *Complaint Investigations System* 87 FR 61649 \(October 12, 2022\)](#), 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.
- 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.

Access and authentication records for FAA employees who use FHWIS are handled in accordance with SORN [DOT/ALL 13, *Internet/Intranet Activity and Access Records* 67 FR 30757 \(May 7, 2002\)](#).

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.

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



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

Accountability and Auditing

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

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

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

In addition to these practices, the FAA consistently implements additional policies and procedures especially as they relate to the access, protection, retention, and destruction of PII. Federal employees/contractors who work with 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 and in FAA Order 1370.121B. The FAA also conducts periodic privacy compliance reviews of FHWIS as related to the requirements of OMB Circular A-130, “*Managing Information as a Strategic Resource*.”

Responsible Official

Anthony Wheat
System Owner
Project Manager, Office of Information & Technology (AIT)



Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

DOT Privacy Office - Approved - 01/13/2025