U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration (FAA)

Enforcement Information System (EIS) & EIS Query and Browse Database (EISQB)

Responsible Official

Lawrence Wade
Email: Lawrence.t.wade@faa.gov
Phone Number: 405-954-7409

Reviewing Official

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

Executive Summary

The Federal Aviation Administration (FAA) developed the Enforcement Information System (EIS) and the EIS Query and Browse Database (EISQB). The EIS application tracks FAA's investigations of statutory or regulatory violations of aviation safety matters nationwide, as well as information about enforcement actions or orders issued. EISBQ is an internal, web-based query and browsing tool that provides Aviation Safety Inspectors (ASIs), Office of Aviation Safety (AVS) and other authorized FAA users read-only access to EIS information.

The FAA previously published the Enforcement Information System (EIS) Modernization Privacy Impact Assessment (PIA) in accordance with the E-Government Act of 2002 because the FAA collects personally identifiable information (PII) from an alleged violator[1] that includes: name, address, telephone number, airmen certification number (if applicable), date of birth, sex, and other PII. FAA updated the EIS & EISQB PIA to include information related to an update of a system of records notice, new data exchanges, and other administrative items.

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

DOT Privacy Office - Approved - 06/4/2025

[1] An alleged violator could be a member of the public, such as an airman, air passenger, or regulated business.
[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).

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 Federal Aviation Act of 1958, as amended, gives the FAA the responsibility to carry out safety programs to ensure the safest, most efficient aerospace system in the world. The FAA is responsible for:

- Regulating civil aviation to promote safety;
- Encouraging and developing civil aeronautics, including new aviation technology;
- Developing and operating a system of air traffic control and navigation for both civil and military aircraft;
- Developing and carrying out programs to control aircraft noise and other environmental effects of civil aviation; and
- Regulating U.S. commercial space transportation.

The FAA's central mission is to promote safety in civil aeronautics. To achieve this, the agency establishes regulatory standards and requirements, found in 14 Code of Federal Regulations (CFR) parts 1-199 under the statutory authority in 49 United States Code (U.S.C.) subtitle VII. Under 49 U.S.C. § 40113, the FAA Administrator has broad authority to take action the Administrator considers necessary to carry out DOT statutory responsibilities and powers relating to safety in air travel, including issuing regulations and standards, conducting investigations, and issuing related orders. The authority to carry out investigations and conduct enforcement proceedings falls under 14 CFR, Part 13 §§ 13.1 – 13.29, 49 U.S.C. §§ 46101 – 46111 Investigations and Proceedings and 49 U.S.C. 44701 – 44735 Safety Regulation.

DOT Privacy Office - Approved - 06/24/2025

Background

The FAA is tasked with promptly and fully investigating, and determining compliance requirement outcomes, for all known or suspected violations of aircraft safety involving airport operation, manufacturing aircraft or aircraft parts, maintaining or operating aircraft, or shipping hazardous materials. These investigations[3] are known as enforcement actions. During the investigation, violations may be identified. In addition, FAA can receive reports of suspected violations from individuals through feedback through FAA-approved reporting tools[4]. The FAA determines during the investigation if a violation occurred or if a reported violation has any merit. In instances where it is determined a violation has occurred or reported violation has merit, the Enforcement Information System (EIS) is used to record and track the violation. EIS serves as the primary database for tracking information about enforcement actions for statutory or regulatory violations concerning the operation and maintenance of aircraft, airports, and aircraft equipment by individual airman, air passengers, or certified companies.

If FAA investigative personnel determine that no violation occurred, they terminate the investigation. Otherwise, if a violation is suspected, the FAA sends an alleged violator a Letter of Investigation (LOI), by U.S. Mail, detailing the alleged violation.

During the investigation, the investigator collects the information directly from the subjects of the investigation via a hardcopy FAA Form 2150-5, "*Enforcement Investigative Report (EIR)*[5]". The EIR is the means for documenting, assembling, organizing, and presenting all evidence and other relevant information obtained during an investigation[6]. The information is then manually entered into EIS per discussion below.

Enforcement Information System

EIS is an internal, web-based application accessible to authorized FAA employees at https://eis.faa.gov/ via their Personal Identity Verification (PIV) card. Investigators access EIS with their PIV card to create an EIR. To track the alleged violation, the investigator enters details related to the violation to create the EIR and the system generates an EIR number[7] which is associated with the record. The investigator manually enters the following

DOT Privacy Office - Approved - 06/24/2025

[3] EIS is not used to conduct or record information pertaining to the investigations.
[4] Please visit https://www.transportation.gov/individuals/privacy/privacy-impact-assessments for a list PIA for FAA information on systems.
[5] The FAA Form 2150-5 is an internal, FAA form that is not publicly accessible nor given to non-FAA personnel for information collection.
[6] If during an investigation, FAA investigative personnel determine that no violation occurred, they terminate the investigation and complete the appropriate sections of the EIR.
[7] The EIR number is a unique number that consists of case year, office code and 4 sequential numbers. The number is used to track the EIR and, once assigned, it never changes.

information, collected on the hardcopy FAA Form 2150-5, into the electronic Form 2150-5 in EIS:

- Full name of alleged violator (certificated individual or business entity);
- Doing business as (DBA) name (business only);
- Designator (business only);
- Alleged violator's mailing address;
- Alleged violator's telephone number;
- Date of birth (DOB);
- Sex;
- Employer's name;
- Airman certificate number (if applicable);
- Certificate type;
- Aircraft, engine, propeller or part involved, make, model, and series (as applicable);
- Aircraft tail number (N-number);
- Aircraft owner's full name and address;
- Region of violation discovery;
- Location of violation (Airport ID);
- Type of violation;
- Investigating field office recommendation (action type and sanction);
- FAA office ID;
- Region; and
- Full name of AFS inspector.

The investigator then enters the airman's certification number and the EIR is populated with the airman's full name, address, sex, airmen's certificate number, and certificate type through a real-time data exchange with the Civil Aviation Information System (CAIS) [8].

Upon completion of the EIR, the investigator submits the EIR to their respective manager for review to ensure accuracy. If the manager finds issues with the information entered by the investigator, the manager transfers the EIR back to the appropriate office for corrections or to provide clarifications. Once the EIR is approved by the respective manager, he/she then decides on the course of action to take for the investigation. There are three possible outcomes for a completed EIR:

- No Action
- Administrative Action

[8] CAIS is a component of FAA's AVS Registry system.

DOT Privacy Office - Approved - 06/24/2025

- Legal Enforcement Action

The EIR for a No Action outcome is closed if it is determined an enforcement action is not required. For Administrative Action, closure of the EIR is done by recommending a corrective action for the violation. For Legal Action, investigations are assigned to the Office of the Chief Counsel (AGC) and all information in the FAA Form 2150-5 is electronically transferred to AGC's Case and Document Management System (CDMS) to determine the appropriate course of legal action.

Enforcement Information System Query and Browse (EISQB)

Authorized users (i.e., Aviation Safety Inspectors (ASIs) and Office of Aviation Safety (AVS) managers) access EISQB at https://eisqb.faa.gov/ using their PIV card. EISQB contains replicated copies of EIS data and provides ASIs, AVS managers, and other authorized FAA users, read-only access to EIS. Authorized users have read-only access to EIRs about airmen, regulated businesses, or air passengers. This provides them access to only the information they need without having to directly access EIS. EISQB users can run queries to look up alleged violation and enforcement information by the EIR number, alleged violator's full name, and/or region and office location.

Streamlined No Action and Administrative Action Process (SNAAP)

SNAAP is a program within EISQB that processes routine administrative letters, for alleged violations, that do not require extensive investigation, do not warrant legal enforcement action, or do not require any action. EISQB receives information from EIS and the National Vital Information System (NVIS) to generate the letters. The letters include the alleged violator's name, mailing address, EIR number, details of the alleged violation, and the inspector's name and business contact information. SNAAP generates the following types of letters:

- No Action (No further action against the alleged violator because of a no violation finding);
- Warning Notice (Administrative action that recites facts about the incident and an indication that an alleged violation may have occurred); and
- 14 Code of Federal Regulations (CFR) 61.15(e) letter - Alcohol or Drug Related Offenses (administrative).

To generate the issuance of a SNAAP, the application pulls the alleged violator's name and mailing address, which is replicated from EIS. The inspector's name and the business

DOT Privacy Office - Approved: 06/24/2025

contact information of the office that created the SNAAP is pulled from NVIS. The authorized user accesses EISQB, enters the EIR number, and downloads the letter generated by SNAAP. That authorized user then mails the letter to the office that originated the EIR for dissemination to the alleged violator.

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[9], 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[10].

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.

During the investigation, the investigator obtains information directly from the alleged violator, witnesses, and others that have information pertaining to the alleged statutory or regulatory violation. The investigator then manually enters information into EIS and includes the alleged violator's name, address, telephone number, airman certification number, date of birth, sex, and aviation employer. The FAA investigator provides verbal notice to those individuals that their information is being collected, pursuant to an ongoing investigation. EISQB does not collect information from individuals but provides its users with read-only access to replicated copies of EIS data, therefore notice is not provided to individuals.

The FAA retrieves records in the EIS by name, certification number and other personal identifiers, and protects Privacy Act records in accordance with the Department's published System of Records Notice, DOT/FAA 847-Aviation Records on Individuals, 89 FR 48956

DOT Privacy Office - Approved - 06/20/2025

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

(June 10, 2024). Records in this system of records notice that relate to administrative actions and legal enforcement actions are exempted from certain access and disclosure requirements of the Privacy Act of 1974, pursuant to 5 U.S.C. 552a(k)(2).

The publication of this PIA demonstrates DOT's commitment to provide appropriate transparency into EIS and EISQB.

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.

EISQB is not a Privacy Act system of records and individuals would exercise their Privacy Act rights through the source records system, EIS. Under the provisions of the Privacy Act, individuals may request searches of EIS to determine if any records have been added that may pertain to them. Individuals wishing to know if their records appear in these systems 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.

Contesting record procedures: Individuals wanting to contest information about themselves that is contained in EIS should make their request in writing, detailing the reasons why their records should be corrected and addressing their letter to the following address:

Federal Aviation Administration
Privacy Office
800 Independence Avenue, SW

DOT Privacy Office - Approved - 06/24/2025

Washington, DC 20591

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

Purpose Specification

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

The FAA's central mission is to promote safety in civil aeronautics. To achieve this, the agency establishes regulatory standards and requirements, found in 14 Code of Federal Regulations (CFR) parts 1-199 under the statutory authority in 49 United States Code (U.S.C.) subtitle VII. Under 49 U.S.C. § 40113, the FAA Administrator has broad authority to take action the Administrator considers necessary to carry out DOT statutory responsibilities and powers relating to safety in air travel, including issuing regulations and standards, conducting investigations, and issuing related orders. The authority to carry out investigations and conduct enforcement proceedings falls under 14 CFR Part 13 §§ 13.1 – 13.29, 49 U.S.C. §§ 46101 – 46111 Investigations and Proceedings, and 49 U.S.C. 44701 – 44735 Safety Regulation.

EIS is used for tracking and managing the investigation of violations affecting aviation safety, and associated FAA enforcement actions and orders. EIS collects the alleged violator's name, address, telephone number, airmen certification number, date of birth, sex, aviation employer and other information discussed in the overview section of this PIA. The information is collected to support FAA's oversight and enforcement of compliance with safety regulations, statutes, and orders. Through a real-time data exchange with CAIS, EIS receives the airman's full name, address, sex, airmen's certificate number, and certificate type and this information is used to populate the EIR. EIS provides CDMS all the information collected on FAA Form 2150-5 through an electronic transfer. The information is used by AGC to determine the appropriate course of legal action.

EISQB provides read-only access to replicated EIS information and this allows authorized users to review current and historical data on FAA enforcement actions against airlines, pilots, and mechanics. SNAAP, a program within EISQB, receives information from EIS and NVIS to generate letters. The SNAAP letters are replicated in EISQB, then downloaded and sent to the originating office for dissemination to the alleged violator.

DOT Privacy Office - Approved - 06/24/2025

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.

EIS collects the minimum amount of PII necessary to document the investigative process, enforcement actions and orders, and violations affecting safety in the National Airspace System.

The previously approved records schedule, N1-237-92-004, Legal Enforcement Case Files and the Enforcement Information System (EIS), is being split into two new records schedules. Legal Enforcement Case Files, N1-237-92-004, item 1, will be covered by DAA-0237-2025-0005-0001, Legal Enforcement Case Files. Disposition: Temporary. Cutoff instructions: Cut off after the case is closed. Retention period: Destroy five years after cutoff. This schedule has been submitted to the National Archives and Records Administration (NARA) and is currently going through their review process. The Enforcement Information System (EIS) records, N1-237-92-004, item 4, will be covered by DAA-0237-2025-0017, Enforcement Information System (EIS). Disposition of these records is to be determined as this records schedule is currently being drafted by the program office and will be submitted to NARA once it is finalized.

EISQB provides authorized users with read-only access to the information from EIS; it does not create or store any records. Lastly, SNAAP letters generated in EISQB will be disposed of as follows: No Action letters after 90 days and Administrative Action letters after 365 days.

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.

EIS collects the alleged violator's name, address, telephone number, airmen certification number, date of birth, sex, aviation employer and other information discussed in the overview of this PIA. The information is used to document investigations, and to process enforcement orders and actions. FAA uses EISQB to provide authorized user access to read-only data in EIS and this allows authorized users to review current and historical data on FAA enforcement actions against airlines, pilots, and mechanics. SNAAP, a program within EISQB, receives information from EIS and NVIS to generate routine administrative letters for alleged violations that do not require extensive investigation, do not warrant legal enforcement action, or do not require any action. The letters include the alleged violator's name, mailing address, EIR number, details of the alleged violation, the inspector's name, and business contact information.

DOT Privacy Office Approved - 06/24/2025

SORN DOT/FAA 847, *Aviation Records on Individuals*, includes the following specific routine uses permitting the sharing of Privacy Act records:

- Provide basic airmen certification and qualification information to the public upon request. Examples of basic information include: the type of certificates and ratings held; the date, class, and restrictions of the latest physical airman's certificate number; the status of the airman's certificate (i.e., whether it is current or has been amended, modified, suspended or revoked for any reason); the airman's home address, unless requested by the airman to be withheld from public disclosure per 49 U.S.C. 44703(c); and requests for review of certificate denials.
- Disclose information to the National Transportation Safety Board (NTSB) in connection with its investigation responsibilities.
- Provide information about airmen to Federal, State, local and Tribal law enforcement agencies when engaged in an official investigation in which an airman is involved.
- Provide information about enforcement actions or orders issued thereunder to government agencies, the aviation industry, and the public upon request.
- Make records of delinquent civil penalties owed to the FAA available to the U.S. Department of the Treasury (Treasury) and the U.S. Department of Justice (DOJ) for collection pursuant to 31 U.S.C. 3711(g).
- Make records of effective orders against the certificates of airmen available to their employers if the airmen use the affected certificates to perform job responsibilities for those employers.
- Make airmen records available to users of FAA's Safety Performance Analysis System (SPAS), including the Department of Defense Commercial Airlift Division's Air Carrier Analysis Support System (ACAS) for its use in identifying safety hazards and risk areas, targeting inspection efforts for certificate holders of greatest risk, and monitoring the effectiveness of targeted oversight actions.
- Provide information about airmen to Federal, State, local, and Tribal law enforcement, national security, or homeland security agencies whenever such agencies are engaged in the performance of threat assessments affecting the safety of transportation or national security.

SORN 847 also includes 15 departmental routine uses.

DOT Privacy Office - Approved - 06/24/2025

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 collects, uses, and retains data that is relevant and necessary for the purpose for which it was collected. The investigator manually enters all information from the FAA Form 2150-5, into EIS and performs a check to ensure the accuracy of the information as it is entered. Additionally, the respective managers check the accuracy of information and returns to the investigator to rectify, if required.

EISQB data is replicated EIS data, so its accuracy depends on EIS. SNAAP, a program within EISQB, receives information from EIS and NVIS to generate letters. The FAA also ensures data accuracy in EIS by conducting annual EIS database reviews. In addition, automated data checks are in place to ensure information entered conforms to the expected values and formats.

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 December 10, 2020).

EIS and EISQB protect PII with reasonable administrative, technical, and physical security safeguards against loss or unauthorized access or compromise of the information. Both applications are only available to authorized FAA employees that access the system using their personal identity verification card.

DOT Privacy Office - Approved - 06/24/2025

FAA personnel adhere to agency-wide procedures for handling and safeguarding PII and receive annual privacy and security training. The system manages access to information through user roles. Users receive the least privileges possible to perform their job duties through the user roles for development, support, and maintenance.

EIS received its current Authority to Operate (ATO) on August 17, 2022, and EISQB ATO was awarded on July 24, 2024.

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 EIS and EISQB 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 EIS and EISQB as related to the requirements of OMB Circular A-130, *"Managing Information as a Strategic Resource."*

DOT Privacy Office - Approved - 08/24/2025

Responsible Officials

Lawrence Wade
EIS System Owner
Office of Solutions Delivery

Kevin Colbert
EISQB System Owner
Office of Solutions Delivery

Prepared by: Barbara Stance, 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: 2025.06.24 10:18:46 -04'00'

DOT Privacy Office - Approved - 06/24/2025