



**U.S. Department of Transportation**  
**Privacy Impact Assessment**  
**Federal Aviation Administration (FAA)**

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

**Responsible Official**

Christine Kim  
EIS System Owner  
Office of Solutions Delivery

**Reviewing Official**

Karyn Gorman  
Acting Chief Privacy Officer  
Office of the Chief Information Officer  
[privacy@dot.gov](mailto: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. EISQB 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<sup>1</sup> that includes: name, address, telephone number, airmen certification number (if applicable), date of birth, sex, and other PII. FAA is updating the EIS PIA to include EISQB because both systems process similar information. The update incorporates and addresses privacy concerns pertaining to EISQB.

### 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.<sup>2</sup>*

*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*

---

<sup>1</sup> An alleged violator could be a member of the public, such as an airman, air passenger, or regulated business.

<sup>2</sup>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 Federal Aviation Administration (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 (C.F.R.) 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 C.F.R. Part 13 §§ 13.1 – 13.29, 49 U.S.C. §§ 46101 – 46111 Investigations and Proceedings, and 49 U.S.C. 44701 – 44735 Safety Regulation.

For any investigations that relates specifically to pilots, the legal authority is 49 U.S. Code § 44703 - Airman Certificates (2) (iii) Pilot Records Database (PRD), that states "The Administrator shall establish an electronic database (in this subsection referred to as the



“database”) containing the following records: (iii) summaries of legal enforcement actions resulting in a finding by the Administrator of a violation of this title or a regulation prescribed or order issued under this title that was not subsequently overturned.”

### *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<sup>3</sup> 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<sup>4</sup>. 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 occurred or a reported violation has merit, EIS is used to record and track the violation. If FAA investigative personnel determine that no violation occurred, they terminate the investigation. The FAA sends 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)*”<sup>5</sup>. The EIR is the means for documenting, assembling, organizing, and presenting all evidence and other relevant information obtained during an investigation<sup>6</sup>. The information is then manually entered into EIS per discussion below.

### *Enforcement Information System*

EIS is an internal, web-based application accessible to authorized AFS employees at <https://eis.faa.gov/> via their Personal Identity Verification (PIV) card. Investigators access EIS with their PIV card to create an EIR. In doing so, the investigator enters details related to the violation to create the EIR for tracking the alleged violation, and an EIR number<sup>7</sup> is generated. The investigator manually enters the following 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);

<sup>3</sup> EIS is not used to conduct or record information pertaining to the investigations.

<sup>4</sup> Please visit <https://www.transportation.gov/individuals/privacy/privacy-impact-assessments> for a list PIA for FAA information on systems.

<sup>5</sup> The FAA Form 2150-5 is an internal FAA form that is not publicly accessible nor given to non-FAA personnel for information collection.

<sup>6</sup> If during an investigation, FAA investigative personnel determine that no violation occurred, they terminate the investigation and complete the appropriate sections of the EIR.

<sup>7</sup> 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.



- Designator (business only);
- Alleged violator's mailing address;
- Alleged violator's telephone number;
- Date of birth (DOB);
- Gender;
- 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 EIR is populated with the airman's full name, address, gender, airman's certificate number, and certificate type through a real-time data exchange with the Civil Aviation Information System (CAIS) <sup>8</sup>.

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 alleged violation investigation. There are three possible outcomes for a completed EIRs:

- No Action
- Administrative Action
- Legal Action

The EIR for No Action 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

---

<sup>8</sup> CAIS is a component of FAA's AVS Registry system.



the Case and Document Management System (CDMS)<sup>9</sup> for AGC to determine the appropriate course of legal action.

*Enforcement Information System Query and Browse (EISQB)*

Authorized users access EISQB at <https://av-info.av.faa.gov/eisqb> 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 would have read-only access to EIRs about airmen, regulated businesses, or air passengers. 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 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);
- Letter of Correction (Alleged violator agrees to take corrective action);
- 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 and the business contact information of the office that created the SNAAP is pulled from NVIS. The authorized user accesses EISQB, enters their 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*

---

<sup>9</sup> CDMS is a workload and work activity tracking system for AGC.





*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<sup>10</sup>, 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<sup>11</sup>.*

## 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 alleged violator, witnesses, or others that have information pertaining to the alleged statutory or regulatory violation. That information is then manually entered into EIS by the investigator 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 receives read-only access to PII, therefore notice is not provided.

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 [Systems of Records Notices, DOT/FAA 847 -Aviation Records on Individuals, 75 FR 68849 \(November 9, 2010\) \(SORN\)](#). 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). EISQB are replicated copies and are therefore not Privacy Act records.

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

<sup>10</sup> <http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf>

<sup>11</sup> [http://csrc.nist.gov/publications/drafts/800-53-Appendix-J/IPDraft\\_800-53-privacy-appendix-J.pdf](http://csrc.nist.gov/publications/drafts/800-53-Appendix-J/IPDraft_800-53-privacy-appendix-J.pdf)



## 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.*

Under the provisions of the Privacy Act, individuals may request searches of EIS and EISQB to determine if any records may pertain to them. Individuals wanting to contest information about themselves, that may be contained in this system, should make their requests in writing, detailing the reasons for why the records should be corrected, to the following address:

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

Included in the request must be the following:

- Name,
- Mailing address,
- Phone number 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 and EISQB should make their requests in writing, detailing the reasons for why the records should be corrected to the following address:

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

## Purpose Specification

*DOT should (i) identify the legal bases that authorize a particular PII collection, activity, or technology that impacts privacy; and (ii) specify the purpose(s) for which it collects, uses, maintains, or disseminates PII. The PII contained in PTB is utilized for transit subsidy usage reconciliation, reporting for the agency, monitoring, and tracking participant usage.*

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 (C.F.R.) 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 C.F.R. Part 13 §§ 13.1 – 13.29, 49 U.S.C. §§ 46101 – 46111 Investigations and Proceedings, and 49 U.S.C. 44701 – 44735 Safety Regulation.

For any investigations that relates specifically to pilots, the legal authority is 49 U.S. Code § 44703 - Airman Certificates (2) (iii) Pilot Records Database (PRD), that states “The Administrator shall establish an electronic database (in this subsection referred to as the “database”) containing the following records: (iii) summaries of legal enforcement actions resulting in a finding by the Administrator of a violation of this title or a regulation prescribed or order issued under this title that was not subsequently overturned.”

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, gender, 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 download and sent to the originating office for dissemination to the alleged violator.

## **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. In accordance with NARA Schedule N1-237-92-004 Enforcement Records, August 10, 1995. Records are maintained as followed:



- Enforcement Records are transferred to the Federal Records Center (FRC) 2 years after the case is closed in EIS. FRC destroys the records 5 years after the case is closed in EIS.
- Cases files resulting in no action are destroyed 30 days after, or no more than 90 days after, the case is closed in EIS.
- Case files resulting in an indefinite suspension of an airman certificate, pending successful completion of reexamination or proof of qualification, are destroyed one month after the date of successful completion of reexamination or proof of qualifications.

The FAA Records Management and Program Office has drafted a replacement records schedule, DAA-0237-2021-0014, to provide a longer retention period (99 years) for airmen records than provided for under NARA, N1-237-92-004. The draft has yet to be submitted or approved by NARA. These records will be retained as permanent until DAA-237-2021-0014 has been approved.

EISQB provides authorized users with read-only access to the information from EIS; it does not create or store any records. All records retrieved, using EISQB, follow the records schedule for EIS. Lastly, SNAAP letters generated in EISQB will be maintained as follows: No Action letters for 90 days and Administrative Action letters for 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 access to 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, inspector's name, and business contact information.

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); information relating to an individual's physical status or condition used to determine statistically the validity of FAA medical standards; and information relating to an individual's eligibility for medical certification, requests for exemption from medical requirements, and requests for review of certificate denials.
- Use contact information to inform airmen of meetings and seminars conducted by the FAA regarding aviation safety.
- 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 through the airmen registry certification system to the Department of Health and Human Services, Office of Child Support Enforcement, and the Federal Parent Locator Service that locates noncustodial parents who owe child support. Records in this system are used to identify airmen to the child support agencies nationwide in enforcing child support obligations, establishing paternities, establishing and modifying support orders and location of obligors. Records named within the section on Categories of Records will be retrieved using Connect: Direct through the Social Security Administration's secure environment.
- Make personally identifiable information about airmen available to other Federal agencies for the purpose of verifying the accuracy and completeness of medical



information provided to FAA in connection with applications for airmen medical certification.

- Make records of past airman medical certification history data available to Aviation Medical Examiners (AMEs) on a routine basis so that AMEs may render the best medical certification decision.
- 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.

The Department has published 15 additional routine uses applicable to all DOT Privacy Act systems of records, including this system. The routine uses are published in the Federal Register at 75 FR 82132, December 29, 2010 and 77 FR 42796, Jul 20, 2012, under “Prefatory Statement of General Routine Uses” available at <http://www.transportation.gov/privacy/privacynotices>).

### 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 address, 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.*



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.

FAA also incorporates standards and practices required for federal information systems under the Federal Information Security Management Act (FISMA) and are detailed in Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, dated March 2006, and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, dated April 2013.

EIS received its current Authority to Operate (ATO) on October 9, 2019 and EISQB ATO was awarded on May 1, 2020.

### **Accountability and Auditing**

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

The FAA's Office of the Chief Information Officer, Office of Information Systems Security, Privacy Division, is responsible for governance and administration of FAA Order 1370-121A, FAA Information Security and Privacy Program and Policy. FAA Order 1370-121A implements the various privacy laws based on the Privacy Act of 1974 (the Privacy Act), the E-Government Act of 2002 (Public Law 107-3470, the Federal Information Security Management Act (FISMA), Department of Transportation (DOT) privacy regulations, Office of Management and Budget (OMB) mandates, and other applicable DOT and FAA information and information technology management procedures and guidance.

In addition to these practices, additional policies and procedures will be consistently applied, especially as they relate to the protection, retention, and destruction of PII. Federal and contract employees are given clear guidance in their duties as they relate to collecting, using, processing, and security privacy data. Guidance is provided in the form of mandatory annual security and privacy awareness training, as well as FAA Privacy Rules of Behavior. The DOT Privacy Office and the FAA Security Compliance Division (AIS-200) will conduct periodic privacy compliance reviews of EIS and EISQB with the requirements of OMB Circular A-130.



### **Responsible Officials**

Christine Kim  
EIS System Owner  
Office of Solutions Delivery

Lawrence Wade  
EISQB System Owner  
Office of Solutions Delivery

Prepared by Barbara Stance, FAA Chief Privacy Officer

### **Approval and Signature**

Karyn Gorman  
Acting Chief Privacy Officer  
Office of the Chief Information Officer

DOT Privacy Office - Approved - 01 05 2022