U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration (FAA)
Office of Finance and Management (AFN)
Instructional Resource Information System (IRIS)

Responsible Official

Barbara King
Email: barbara.king@faa.gov
Phone Number: 405-954-3920

Reviewing Official

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

Executive Summary

Instructional Resource Information System (IRIS) is a Federal Aviation Administration (FAA) Office of Finance and Management (AFN) portal comprised of multiple applications that are focused on eLearning, providing the information needed for students to attend training, and automating the processes of the FAA Academy. The Academy, located at the Mike Maroney Aeronautical Center, Oklahoma City, Oklahoma, provides technical and managerial training and development for FAA employees/contractors who wish to attend offered classes. The system is authorized under 49 United States Code (U.S.C.) § 322, 40122(g), 106 (f)(2), 114(d), 301, 5314, 5315, 20108, 30182, 40108, and 40101; 40 U.S.C. § 1441 and 486c; 5 U.S.C. § 301; 23 U.S.C. § 504; *The National Security Act of 1947*, as amended; *The Homeland Security Act of 2002* (Pub. L. 107–296), dated November 25, 2002; Executive Order (E.O.)12148, *Federal Emergency Management*, dated July 20, 1979, as amended; E.O. 12656, *Assignment of Emergency Preparedness Responsibilities*, dated November 18, 1988, as amended; E.O. 13286, *Establishing the Office of Homeland Security*, dated February 28, 2003, and Title 32 Code of Federal Regulations (C.F.R.).

This Privacy Impact Assessment (PIA) is developed in accordance with Section 208 of the E-Government Act of 2002, because IRIS maintains Personally Identifiable Information (PII) on members of the public (FAA Academy students and their emergency contacts) and information on FAA employee/contractors who manage the IRIS system.

DOT Privacy Office - Approved - 06/13/2025

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]

[1]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).

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

IRIS is authorized under 49 U.S.C. § 322, 40122(g), 106 (f)(2), 114(d), 301, 5314, 5315, 20108, 30182, 40108, and 40101; 40 U.S.C. § 1441 and 486c; 5 U.S.C. § 301; 23 U.S.C. § 504; *The National Security Act of 1947*, as amended; *The Homeland Security Act of 2002* (Pub. L. 107–296), dated November 25, 2002; Executive Order (E.O.)12148, *Federal Emergency Management*, dated July 20, 1979, as amended; E.O. 12656, *Assignment of Emergency Preparedness Responsibilities*, dated November 18, 1988, as amended; E.O. 13286, *Establishing the Office of Homeland Security*, dated February 28, 2003, and Title 32 C.F.R.

IRIS is an AFN component of the FAA Academy and provides the FAA with the applications, programs, databases, and websites necessary to facilitate training. In addition, IRIS contains many components including storage area networks (SAN), virtual hosting servers, backup devices and networking hardware.

Typical transactions within the system include:

- Potential students requesting information regarding courses at the FAA Academy.
- Students being notified of available courses.
- Welcome packages sent to students.
- FAA Academy course evaluation by students.

IRIS on premise components

Computer Managed Instruction (CMI) Application):

DOT Privacy Office - Approved - 06/03/2025

The CMI application provides a course creation environment for the Distance Learning Program Management Office (DLPMO) Government Off-The-Shelf (GOTS) program, CMI, and additional training courses being offered by the FAA. Training materials are provided to DLPMO by authorized Air Traffic Organization and FAA training content providers. Once received, DLPMO developers organize and format the material into training modules. These modules are tested and verified to ensure compatibility with the various field site operating systems. DLPMO then delivers the training modules to the field site once the testing and verification is complete. Distance Learning Platform (DLP) Workstations are used to access the training material in the field sites.

Federal Information Superhighway for Training (FIST):

FIST is a web-based application and a reporting tool of tightly integrated systems, processes and servers. It provides user maintenance interfaces while delivering training reports to various organizations [FAA Academy - Technical Operations (AMA-400), Technical Operations - field offices, and Washington offices].

Integrated Data Protection Appliance (IDPA):

The IDPA provides a solution for data protection administrators who manage independent and disconnected applications to configure and manage data protection and storage devices.

IDPA System Manager enables administrators to efficiently manage the IDPA components from a single user interface—including monitoring, reporting, analytics, and search—to simplify the data protection experience.

The IDPA provides easy configuration and integration of data protection components in a consolidated solution and offers the following:

- Simplified deployment and configuration
- Backup administration
- Deduplication
- Native cloud disaster recovery (DR) and Long-Term Retention (LTR)
- Instant access and restore
- Monitoring and analytics
- Search
- Scalability
- Unified support

SharePoint:

SharePoint is the repository for courseware content.

Virtual Desktop Infrastructure VDI/ IGO:

DOT Privacy Office - Approved - 06/03/2025

VDI/IGO is a virtual desktop that provides rapid deployment of student workstations. Desktop virtualization is used in conjunction with application virtualization within the training environment to provide a comprehensive desktop environment. All the components of the desktop are virtualized, which allows for a highly flexible and much more secure desktop delivery model.

IGO refers to the Citrix appliance which hosts the igo.faa.gov website which is used to authenticate VDI users.

IRIS components in the Federal Cloud Service (FCS) cloud

Academy Catalog of Training (ACT):

ACT is a searchable listing of current courses offered by the FAA and the FAA Academy. The catalog contains a section providing cost of courses for student reference. This is available through the iPhone application.

Academy Evaluation System (AES):

AES is a web application evaluation system for all Academy resident offerings. The application provides for intermediate, end, and post evaluations. AES provides access to instructors and managers to view student feedback for quality management operations.

Academy Student Information System (ASIS):

ASIS is used to provide students that are attending training a welcome packet, a parking pass (the pass will be verified and stamped by the MMAC Security Guard), and information about the Mike Monroney Aeronautical Center (MMAC) and surrounding Oklahoma City area.

Academy Training Platform (ATP) Production, ATP Development, ATP Test:

Websites for ASIS, Azure DevOps, Centrally Billed Account (CBA), Computer Based Instruction (CBI), eTesting, and SSHAT Admin are housed within ATP.

Public Websites for Applications:

This is used for websites that are public facing: ACT, SSHAT, AES, Splash/Redirect pages for eLMS.

Azure DevOps (formerly known as Team Foundation Server (TFS):

Azure DevOps is a Commercial Off-The-Shelf (COTS) application for change management tracking used by the IRIS Support Team to manage changes within the IRIS system.

Centrally Billed Account (CBA) Central Billing Account:

The Student Services CBA provides a form for logging payments for the Air Traffic Control Specialist new hire students.

DOT Privacy Office - Approved - 06/03/2025

Computer Based Instruction (CBI) Property Management Website:

The CBI Property Management website maintains information on field site hardware and equipment, and the contact numbers for those sites. The CBI Property Management Website collects information required to identify each of the field site systems and computer operating system versions. Information relating to an individual is not retrievable by a unique identifier. Platforms are identified by machine or site identifiers. Once the platform is identified, the administrator's information for that platform is visible.

Databases (Production, Test and Development):

There are three (3) instances of databases: development, test and production. Databases for the ATP.

Digital Signage:

Automated electronic messaging board at the Mike Monroney Aeronautical Center (MMAC) that displays weather information, MMAC announcements and events.

Electronic Learning Management System (eLMS) Content:

The eLMS content servers provide FAA and Department of Transportation (DOT) with storage for their on-line training content for use with the eLMS system. eLMS have a security authorization outside of IRIS' security boundary. The on-line training content is owned by the content creators, not IRIS or AMA-24. There are two (2) eLMS Content servers: Production and Staging. No student/personal information is stored on the eLMS Content servers. eLMS Content is currently operating in a hybrid mode with On Prem and Cloud servers/services.

eTesting:

eTesting is a web-based application that dynamically generates course examinations for the training instructors at MMAC.

Student Services Housing and Transportation (SSHAT):

SSHAT is a website with information for students who are attending classes at the MMAC. This site provides current registered housing options and information about transportation options to and from MMAC. This is available through the iPhone application.

DOT Privacy Office - Approved - 06/03/2025

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[2], 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[3].

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.

IRIS is a privacy-sensitive system because it collects and maintains PII (name, email address, phone number, and home address) on members of the public (students) that request information for the FAA Academy services. These users provide their PII by filling out the form on the FAA Academy website at Uniform Resource Locator (URL) https://academy.faa.gov/catalog/cpnt. IRIS also collects PII (name, email address, phone number, and home address) on the members of the public (emergency contacts for FAA academy students).

A Privacy Act Statement (PAS) discussing the Department's privacy practices, regarding the collection, use, sharing, maintenance, and disposal of their PII is provided by the Agency/Department at the initial point of collection.

The Department also provides general notice to the public of these records collection through the following Privacy Act System of Records Notices (SORN):

- DOT/ALL 9 *Identification Media Record Systems*, 67 FR 62511 (October 7, 2002) covers applications, photographs, receipts for DOT identification and verification media and official credentials, temporary building passes, security badges, security clearance level and type, date of clearance, clearance basis, entry on duty information, current duty assignment information, routing symbols, limited relevant portions of the media in a manner less secure than its original source records about

DOT Privacy Office - Approved - 06/03/2025

students that provides contact information. The records may include the following PII about students: name, email address, phone number, and home address.

- DOT/ALL 22 *Emergency Contact Records (ECR) Not Covered by Notices of Other Agencies* 75 FR 68852 (November 9, 2010) covers records containing personal contact information for students and for their designated contacts and to notify the designated contact in the event of an emergency. The records may include the following PII about emergency contacts for students: name, email address, phone number, and home address.

- DOT/ALL 27 *Training Programs* 83 FR 60960 (November 27, 2018) covers individual's name, individual's date of birth, student or other identification number assigned to the individual address, phone number, email address, employer name, address, and contact information, occupation/job title, resume/qualifications (for course instructors) applications, registration form, course rosters and sign-in sheets, instructor lists, payment records, including financing, travel and related expenditures, grades and student evaluations, course evaluations, examination and testing materials, and other records and reports related to training. The records may include the following PII about students: name, email address, phone number, and home address.

- DOT/ALL 13 *Internet/Intranet Activity and Access Records* 67 FR 30757 (May 7, 2002) covers records and reports including Internet/Intranet Protocol (IP) address of the computer used to make the Internet/Intranet connection, logs of Internet/Intranet access and use from a DOT computer generally do not directly contain names or similar personal identifiers. However, for official government business purposes and through research or investigation, an individual whose PC was assigned an IP address at a given time may be identifiable by name. The records may include the following PII about students: name, email address, phone number, and home address.

The publication of this PIA demonstrates DOT's commitment to providing appropriate transparency into the IRIS 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.

Each student has the ability to correct their name, email address, phone number, and designated emergency contact information related to themselves at any time by navigating the IRIS URL https://academy.faa.gov/catalog/Home/Contact/ and contacting the IRIS program/administrator.

For all inquiries related to the information contained in IRIS 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.

DOT Privacy Office - Approved - 06/03/2025

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 information collected and maintained in IRIS is authorized under 49 U.S.C. § 322, 40122(g), 106 (f)(2), 114(d), 301, 5314, 5315, 20108, 30182, 40108, and 40101; 40 U.S.C. § 1441 and 486c; 5 U.S.C. § 301; 23 U.S.C. § 504; *The National Security Act of 1947*, as amended; *The Homeland Security Act of 2002* (Pub. L. 107–296), dated November 25, 2002; Executive Order (E.O.)12148, *Federal Emergency Management*, dated July 20, 1979, as amended; E.O. 12656, *Assignment of Emergency Preparedness Responsibilities*, dated November 18, 1988, as amended; E.O. 13286, *Establishing the Office of Homeland Security*, dated February 28, 2003, and Title 32 C.F.R.

IRIS maintains members of the public (for example, students) PII (name, email address, phone number, and home address) of those who request information for academy services by filling out the form on the website at URL https://academy.faa.gov/catalog/cpnt. After a

student is enrolled at the FAA Academy, IRIS collects the name, email address, phone number, and home address of the emergency contacts for students taking courses at the FAA Academy.

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 use the IRIS program and/or manage the system. This use is consistent with the description in the "purpose" section in the applicable system of records notice, DOT/ALL 13, *Internet/Intranet Activity and Access Records,* 67 FR 30757 (May 7, 2002).

IRIS uses this information in accordance with the purposes for which it is collected: for access and authentication to the system for DOT/FAA employees and contractors. This information is used in accordance with the description in the "Purpose" section of SORN DOT/ALL 9 *Identification Media Record Systems*, 67 FR 62511 (October 7, 2002).

IRIS uses this information in accordance with the purposes for which it is collected: To manage, oversee, and document training provided to DOT employees and contractors. This information is used in accordance with the description in the "Purpose" section of SORN DOT/ALL 27 *Training Programs* 83 FR 60960 (November 27, 2018).

IRIS uses this information in accordance with the purposes for which it is collected: For the FAA to notify the designated third-party contact(s)/emergency contact of a FAA employee or contractor in case of an emergency. This information is used in accordance with the description in the "Purpose" section of SORN DOT/ALL 22 *Emergency Contact Records (ECR) Not Covered by Notices of Other Agencies* 75 FR 68852 (November 9, 2010).

The PII in the IRIS 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 provide course information to students. The FAA collects the minimum amount of information from individuals to support providing contact information for students and their designated emergency contacts to the FAA Academy if an emergency occurs.

DOT Privacy Office Approved: 05/08/2025

The FAA maintains different types of records in accordance with following National Archives and Record Administration (NARA) approved General Retention Schedules[4] (GRS):

- Training Correspondence File records are maintained under NC-237-75-3, *Personnel and Training Activities,* Item 3(b). These records are temporary**.** Destroy after five years.

- Training Program File records consisting of correspondence, reports and related document reflecting to 1) training in aviation professional skills; b) technical and management training; c) employee development; and d) direction and supervision of FAA schools, maintained by the Office of Personnel and Training are maintained under NC-237-75-3, *Personnel and Training Activities*, Item 4. These records are temporary. Destroy after five years.

- Information Technology Operations and Maintenance Records Information Technology Operations and Maintenance records are maintained under NARA GRS 3.1, *General Technology Management Records*, Item 020. These records are temporary. Destroy 3 years after help desk tickets are completed. Destroy 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use.

- Authentication and access records are covered under NARA GRS *Systems Security Records, September 2016, Item 030*, are temporary and should be destroyed when business use ceases.

Use Limitation

DOT shall limit the scope of its PII use to ensure that the Department does not use PII in any manner that is not specified in notices, incompatible with the specified purposes for which the information was collected, or for any purpose not otherwise permitted by law.

The FAA limits the scope of PII it collects to what is necessary to meet business needs including:

- First and last name
- Email address
- Phone number

[4] 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 in order to promote consistent retention practices.

DOT Privacy Office - Approved - 06/03/2025

- Home address

The list of PII above is used for communicating with students and their designated emergency contacts.

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

- DOT/ALL 13, *Internet/Intranet Activity and Access Records,* 67 FR 30757 (May 7, 2002)
- DOT/ALL 9 *Identification Media Record Systems*, 67 FR 62511 (October 7, 2002)
- DOT/ALL 27 *Training Programs* 83 FR 60960 (November 27, 2018)
- DOT/ALL 22 *Emergency Contact Records (ECR) Not Covered by Notices of Other Agencies* 75 FR 68852 (November 9, 2010)

The Department has also published 15 additional routine uses that apply to all DOT Privacy Act systems of records, including this system. These routine uses are published in the Federal Register at 75 FR 82132, December 29, 2010, 77 FR 42796, July 20, 2012, and 84 FR 55222, October 15, 2019 under "Prefatory Statement of General Routine Uses."

Finally, the FAA periodically reviews the collection and use of PII through its annual review of this PIA, a Privacy Threshold Analysis (PTA), and Privacy Continuous Monitoring (PCM) document.

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 IRIS data. IRIS data are encrypted at rest and in transit. IRIS 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.

IRIS operates in accordance with DOT Order 1351.37, Departmental Cybersecurity Policy which requires:

- All DOT information systems that are subject to the Federal Information Security Management Act (FISMA) must undergo continuous monitoring of the security controls of the information system;

DOT Privacy Office - Approved - 06/13/2025

- The results of the continuous monitoring are to be reported to the Authorizing Official (AO) on at least an annual basis to communicate any changes in the risk posture of the information system; and
- The AO, with assistance of the Information System Owner (ISO), Risk Executive and other DOT component personnel, review risk posture and planned corrective actions for reducing risk to make a determination if risk is acceptable for continued operation.

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 the IRIS 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 IRIS. 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 IRIS an on-going authorization to operate.

The following safeguards are designed to ensure the security, integrity, and confidentiality of PII in IRIS:

- Encryption of PII which is stored and/or transmitted is compliant with FIPS 140-2 standards.
- IRIS personnel handling sensitive information are required to undergo appropriate background checks to assess their suitability to perform in public trust positions.

DOT Privacy Office - Approved - 06/03/2025

Additionally, all staff undergoes initial security awareness training and annual refresher training, and the procedures for properly protecting the privacy of users' personal information are stressed in this training.

IRIS is designed to meet all current cyber security requirements for protecting privacy information while still allowing only authorized users the full transparency needed to complete the personnel security process for applicants, employees, and contractors. IRIS records are safeguarded in accordance with applicable rules and policies, including all applicable Department automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored.

Access to the computer system containing the records in IRIS is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances and permissions. IRIS is protected from unauthorized access through appropriate administrative, physical, and technical safeguards and all system access is logged and monitored.

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 is responsible for identifying, training, and holding Agency personnel accountable for adhering to FAA privacy and security policies and regulations. 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 IRIS 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.

DOT Privacy Office - Approved - 10/13/2025

The FAA also conducts periodic privacy compliance reviews of IRIS as related to the requirements of OMB Circular A-130, "*Managing Information as a Strategic Resource*."

Responsible Official

Barbara King
Information System Owner
Division Manager, AMA-020

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN MARIE GORMAN
Digitally signed by KARYN MARIE GORMAN
Date: 2025.06.03 15:05:11 -04'00'

DOT Privacy Office - Approved - 06/03/2025