U.S. Department of Transportation

Privacy Impact Assessment (PIA)

Federal Aviation Administration (FAA)
Security and Intelligence (ASH)
Investigations Tracking System (ITS)

Responsible Official

Atul Celly
Email: ASH-AXM-AppSupportTeam@faa.gov
Phone Number: 1-888 584-8334

Reviewing Official

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer



Executive Summary

The Federal Aviation Administration (FAA) Security and Intelligence (ASH) Investigations Tracking System (ITS) is a web-based application used to conduct three different types of investigations: Personnel Security Investigations, Internal Investigations, and Regulatory Investigations. ITS operates under the following authorities: 49 United States Code (U.S.C.), chapter 449, *Air Transportation Security*, enacted as Pub. L. 103–272 on July 5, 1994; *The Transportation Safety Act of 1974*; FAA Drug Enforcement Assistance Act of 1988; *Executive Order* (EO) 10450 (Security Requirements for Government Employment); EO 12968 *Access to Classified Information*; and EO 12829 *National Industrial Security Program.*

The FAA is publishing this Privacy Impact Assessment (PIA) update for the Investigations Tracking System (ITS) in accordance with Section 208 of the E-Government Act of 2002 because the system collects and processes Personally Identifiable Information (PII) from members of the public, including pilots, aircraft owners, mechanics, job applicants, and non-employees needing access to FAA facilities, including those that have applied for employment with the FAA, applied for access to FAA facilities/resources/information, or have been the subject of a complaint or investigation. This update includes changes to the System of Records Notices (SORNs), National Archives and Records Administration (NARA) records disposition schedules (GRS), and authorities for which ITS operate under.

What is a Privacy Impact Assessment?

The Privacy Act of 1974 articulates concepts for how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The assessment is a practical method for evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed. The PIA is an analysis of how information is handled to—i) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; ii) determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and iii)examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[1]

Conducting a PIA ensures compliance with laws and regulations governing privacy and demonstrates the DOT's commitment to protecting the privacy of any personal information

[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).

DOT Privacy Office Approved - 10/22/2020

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

The ASH Office of Personnel Vetting (AXP) processes suitability background investigations for FAA employees, contractors, pilots, aircraft owners, aircraft mechanics, job applicants, and non-employees who need access to FAA facilities. The ASH Office of Investigations & Professional Responsibility (AXI) also conducts investigations into alleged employee misconduct; FAA insider threat analysis; alleged criminal activity by airmen and other FAA certificate holders; unapproved aircraft parts; counterfeit certificates; falsification of official documents; security violations; property theft; laser incidents; unmanned aircraft system incidents; and other investigative services provided to law enforcement agencies. The FAA is able to complete these actions by utilizing the ITS, which is a secure, online repository of sensitive, unclassified information that helps the FAA fulfill its mission and responsibilities to process personnel security investigations, investigate employee misconduct, criminal activity by airmen and other certificate holders, and process civil/tort, administrative, and regulatory investigations against the FAA.

The ITS consists of three different modules/functionalities: Personnel Security investigations; Internal investigations; and Regulatory investigations.

Personnel Security Investigations – ITS is used to track background investigations for FAA employees, contractors, and members of the public.[2] The PII comes to ITS in varying business processes detailed below.

All applicants (new FAA employees, new FAA contractors, and new non-employees) fill out one of the following Office of Personnel Management (OPM) forms to include Standard Form (SF)-85 *Questionnaire for Non-Sensitive Positions*, SF-85P *Questionnaire for Public Trust Positions*, or SF-86 *Questionnaire for National Security Positions.* The Office of

[2] Members of the public include potential FAA and contract employees, non-employees, airmen, other FAA certificate holders, and law enforcement.

DOT Privacy Office - Approved - 10/22/2026

Personnel Security (AXP) Personnel Security Specialist (PSS) then enters the information from the forms into ITS.

ITS Personnel Security Investigation Process:

Step 1 – Initiation

AXP initiates the background investigation process when an AXP PSS or FAA sponsor sends an email to the applicant with detailed instructions for completing and submitting the online questionnaire, fingerprinting, and other required investigative forms for the suitability clearance.

Initiation of the background investigation happens in one of three ways:

- **FAA employees** [from the FAA Office of Human Resources (AHR)] – FAA AHR initiates a personnel security background investigation request for a new FAA employee. The new FAA employee fills out one of the above applicable forms based on their job type. The PII comes via a data exchange with AHR and is stored and maintained in ITS.
- **Non-Employees Access Portals**[3] (NEAP) – The FAA sponsor for the company/state, local, and federal agencies uses NEAP to initiate a personnel security background investigation request for non-employees. The non-employee completes one of the applicable forms above for their job type. The sponsor logs then stored and maintained in ITS.
- **Contractor Personnel** -Vendor Access Portal (VAP2) – Contractor companies that have a contract with the FAA use VAP2 to initiate a personnel security background investigation request. The new FAA contractor applicable forms above for their job type. VAP2 is then used to upload the contractor's PII, which is stored and maintained in ITS.

The following PII is collected for all background investigations from the above processes as part of Personnel Security Investigations:

- Full Name
- Social Security Number (SSN)
- Date of Birth (DOB)
- Suffix
- Security Office
- Position
- Line of Business (LOB)
- City of Birth
- State of Birth
- Country of Birth

[3] NEAP and VAP2 are subsystems within ITS.

DOT Privacy Office - Approved 10/22/2015

- Proposed Start Date
- Date Questionnaire for Investigation Processing (eQIP) Initiated
- Contracting Officer (CO)/Contracting Officer Representative (COR) Name*
- CO/COR Email Address*
- Contract Number*

*Only collected for FAA contractors.

Step 2 – Submission

Current and potential Federal employees, contractors, and non-FAA employees fill out one of the following Office of Personnel Management (OPM) forms: *Standard Form (SF)-85 Questionnaire for Non-Sensitive Positions; SF-85P Questionnaire for Public Trust Positions; or SF-86 Questionnaire for National Security Positions* for their background investigations during the employment eligibility process in addition to the Questionnaire for Investigation Processing (eApp) system, which provides fingerprints and submission of other applicable forms back to the AXP PSS.

Note: Defense Counterintelligence and Security Agency (DCSA) National Background Investigations Service (NBIS) eApp (electronic application) are the new entry point for background investigation applications and is replacing eQIP as the system for initiating investigations. eApp contains the investigative Standard Forms (SFs) that federal applicants and employees use to enter the information required to process their personnel background investigations.

Step 3 – Interim Decision[4] Upon receipt of all required forms and the results of a fingerprint check from the Federal Bureau of Investigation (FBI), the AXP PSS reviews the forms and other available information to determine if an applicant/employee can be placed into the requested position pending the completion of the full background investigation.

Step 4 – Investigation

The DCSA conducts the actual background investigation, where the data is uploaded by the AXP PSS to the eAPP system. The investigation process includes record searches, employment and education verifications, reference checks, and file reviews. Depending on the type of investigation, the applicant/employee may be contacted by a DCSA investigator for a subject interview, and the applicant/employee's neighbors, colleagues, employers, and/or references may also be interviewed.

Step 5 – Adjudication

After the applicant/employee background investigation is completed by DCSA and transmitted to the FAA via data exchange with the eDelivery/Connect Direct System (eDelivery), AXP reviews and adjudicates the background investigation. The

[4] Applies only to applicants/employees moving to a new position.

DOT Privacy Office - Approved - 10/22/2026

applicant/employee may be asked by an AXP PSS to provide additional information during the adjudication process. Although uncommon, if there are significant critical issues that cannot be mitigated, AXP will refer federal applicant cases to the Office of Human Resources (AHR) for a final suitability determination. For issues that may arise with contractor cases, AXP makes the final suitability determination. In all cases, the applicant/employee is provided an opportunity to address critical information prior to a final determination. Employee reinvestigations that disclose potential violations of FAA Standards of Conduct are referred to the Labor and Employee Relations office for review and appropriate action.

Clearance Document Operating Tool (CDOT) - The Clearance Document Operating Tool (CDOT) is an application designed to streamline the management and processing of personnel clearance documentation within facilities. It enables facility managers to securely upload critical forms, such as the SF-312 (Classified Information Nondisclosure Agreement), into a centralized system. Once uploaded, these documents are routed into a dedicated processing queue where they undergo validation and review to ensure completeness and compliance with security requirements. After successful verification, the documents are integrated into the ITS2 system for official recordkeeping and future reference. By automating and organizing this workflow, CDOT enhances efficiency, reduces manual errors, and ensures that clearance documentation is properly tracked and maintained.

Visit Authorization Request System (VARS) - The VARS is a platform that facilitates the coordination and approval of visit requests between FAA program offices and external agencies. It allows FAA users to submit, track, and manage requests for personnel visits, ensuring that all necessary security and administrative requirements are met prior to granting access. VARS supports both inbound and outbound visit requests, providing a standardized process for communication and authorization across organizations. The system helps program offices efficiently review requests, verify visitor credentials, and maintain accurate records of authorized visits. By centralizing this process, VARS improves transparency, reduces processing time, and strengthens compliance with security protocols.

Additionally, as part of the investigative process, an AXP PSS may manually enter data into ITS that they have collected verbally through interviews with the individual, reviews of records provided by the individual, as well as from other Federal, State, tribal, local, and foreign investigative and law enforcement agencies, and other authorized applicable investigative techniques. The AXP PSS provides the ITS Privacy Act Statement (PAS) to individuals from whom they collect PII. ITS receives and sends information from/to external and internal FAA systems to support the FAA's personnel and security investigative efforts and to record the investigation outcome.

DOT Privacy Office - Approved - 10/22/2026

Internal Investigations

The second type of investigations within the ITS track internal FAA investigations involving the following types of allegations: FAA employee, contractor, and non-employee misconduct, falsification of official documents, security violations, tort claims against the FAA, property theft, and reports on administrative investigations on cases related to conduct and discipline matters. All internal investigations are handled in the Busser Investigation Management System[5] (BIMS), a subsystem within ITS.

Internal Investigation Business Process:

Step 1 – National Case Intake Portal[6] (NCIP) Submission

An internal investigation begins when a manager logs into the NCIP, fills out a request,[7] and reports alleged employee misconduct, which is maintained in BIMS. The request contains the individual's name, FAA email address, routing code, position title, office, and FAA phone number. The electronic submission allows for centralized receipt, allegation evaluation, investigative assignment, and transfer of data to the official investigative system of record for the Agency. BIMS does not share the outcome of the investigation with other systems; however, information may be shared with the Office of the Chief Counsel (AGC), or others involved with the resolution of the investigation.

Step 2 – Review Submission

Office of Investigation (AXI) intake group reviews the reported issue submitted from the NCIP and decides whether they fall within AXI's jurisdiction for conducting an investigation.

Step 3 – Refer

Upon completing the review of the submission, a decision is made to refer the issue(s) that are not within the ASH/AXI jurisdiction to the appropriate agencies and/or FAA Line of Business (LOB) with jurisdiction to review the matter.

Step 4 – AXI Assigned

If the allegation falls within the ASH jurisdiction, the AXI intake group assigns an AXI Special Agent to conduct non-criminal investigations. ASH refers all criminal matters to the investigative agency with jurisdiction over those allegations.

Step 5 – Investigation Guidance

Investigations are done according to the guidance in AXI's programs under AXI intake, Security and Hazardous Materials (SH) Order 1600.20, and all applicable FAA and

DOT Privacy Office - Approved - 10/22/2026

[5] BIMS is a subsystem within ITS.
[6] NCIP is a subsystem within ITS.
[7] Individuals may report potential violations through a variety of methods such as the FAA Hotline, Whistleblower or through their manager.

Department of Transportation (DOT) orders.

Step 6 – Investigation Offices

Investigations are conducted by the Internal Investigation Division (AXI-100), Investigative Services Division (AXI-200); and Office of National Security & Enforcement (AXT). All final investigation results go through an approval process, the requester is briefed, and then the investigation is closed out. A report is sent to the requester that summarizes the investigation findings.

International Traveler Security Program (ITSP):

The International Traveler Security Program Dashboard (ITSP) was added to provide a single interface for managing all international traveler functions when FAA employees travel internationally on behalf of the FAA. The program provides international travelers with pertinent information, including a country risk profile list, alerts, the ability to join the mailing list on international travel, security events, travel follow up questionnaire, news, and the ability to fill out the International Traveler Information Card (ITIC) Form, and more.

The ITIC is a form where FAA employees register and provide PII to create a personal profile of themselves, which includes LOB group, FAA office address, FAA phone number, government furnished equipment (GFE) mobile number, personal and FAA email, physical description (height, weight, eye color, shoe size, shirt size, pants size, tattoos, blood type, ethnicity, and duress word or “personal authenticator statement"). This is all optional information that the traveler can submit when traveling internationally for the FAA in case there is an emergency/necessity to go in a retrieve the employee. There is also a List Server (Mailing List) feature that is optional for FAA employees where they provide their name, FAA email, and GFE phone number to receive any information related to planned or current international travel threats. Further, there is a follow-up questionnaire related to any security incidents incurred during travel.

The ITIC Form used by the International Travel Security Branch (ITSB) contains PII, such as name, email address, phone number, DOB, and the above-mentioned biometric data.

Regulatory Investigations

The third type of investigation in ITS is regulatory investigations. The Regulatory Investigation Tracking System (RITS), a subsystem within ITS, is used to track regulatory investigations involving the following types of allegations: Certificate Holder driving under the influence (DUI)/ driving while intoxicated (DWI), Laser/Unmanned Aircraft Systems (UAS) Incidents, and Law Enforcement Assistance Program (LEAP) investigations.

Program Business Processes:

- DUI/DWI Program. The DUI/DWI Program investigates intentional falsifications and incorrect statements on applications for airman medical

DOT Privacy Office - Approved: 10/22/2026

certification involving DUI/DWI entries. It investigates the failure of pilot certificate holders to timely provide reports of motor vehicle actions involving the operation of a motor vehicle while intoxicated, impaired, or under the influence of alcohol or drug. The DUI/DWI program keeps the FAA apprised of motor vehicle actions involving pilots who hold airman medical certificates and actions involving pilots operating certain small aircraft without an airman medical certificate under 14 C.F.R. part 68. This information is submitted from the airman on the Notification Letter Application and includes the airman's name, address, DOB, Airman Certificate Number, and state and date of arrest.

- Law Enforcement Assistance Program (LEAP). The FAA LEAP responsibilities include providing assistance to federal, state, local, foreign, and other law enforcement agencies when their investigations involve areas of FAA regulatory responsibility, such as the transportation of prohibited drugs by aircraft, aviation-related criminal acts, and threats to national security. LEAP investigates falsifications on applications for airman certificates, including airman medical certificates, involving felony and misdemeanor convictions. LEAP also investigates aircraft registration violations. PII involved with LEAP investigations includes an individual's (subject, witness, airman, etc.) name, DOB, address, company name, and aircraft owner details.
- Laser /UAS Events. This module tracks and coordinates investigations into Laser and UAS incidents. A Common Separated Variables (CSV) file is sent from ASH AXE-100 via email and manually uploaded into ITS. The CSV file contains longitude, latitude, airport name, law enforcement, etc., and other fields. When the file comes to ITS, it usually does not contain PII; however, it could contain the UAS registration information.

DOT Privacy Office Approved - 10/22/2025

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 National Institute of Standards and Technology (NIST), Special Publication 800-122. The Office of Management and Budget (OMB), and the Federal Chief Information Officers Council and the Privacy Controls articulated in the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations.[8]

Transparency

Sections 522a(e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act

[8] https://csrc.nist.gov/publications/detail/sp/800-53a/rev-5/final

require public notice of an organization's information practices and the privacy impact of government programs and activities. Accordingly, DOT is open and transparent about policies, procedures, and technologies that directly affect individuals and/or their personally identifiable information (PII). Additionally, the Department should not maintain any system of records the existence of which is not known to the public.

The FAA employs multiple techniques to ensure that individuals are informed of the purpose for which the FAA collects, uses, disseminates, and retains their PII within ITS. For an individual's PII to be included in the system, the individual must have applied for employment with the FAA, applied for access to FAA facilities/resources/information, or have been the subject of a complaint or investigation. With respect to information received through interviews, review of records, and other authorized applicable investigative techniques, the individual being interviewed is provided with a Privacy Act Statement (PAS) that is issued from the AXP PSS during the investigative interview, whether they are the subject of the investigation or are providing content for the investigation. The PAS describes the purpose, details the authority under which the PII is collected, and the results if the individual does not provide the requested information. The collected PII is only used for the purpose for which it is collected.

FAA employees, contractors, and job applicants also review a PAS on SF 85, SF 86, and DOT Form 1681 *Identification Card/Credential Application* when they apply for jobs at the FAA or request a FAA identification badge. These forms provide notice to individuals that the agency has published notice in the Federal Register describing the system of records in which the records will be maintained. This notifies employees, contractors, and applicants of the scope of information requested, the routine uses and allows them to consent or decline to provide the information.

Lastly, employment applicants consent to submission and release of PII when they complete the employment application forms to apply for FAA jobs.

ITS is the FAA's official repository for investigations and the records are covered by the Privacy Act. PII contained in ITS includes, but is not limited to, name, DOB, age, gender, place of birth, and SSN and these records are handled in accordance with the Department's published System of Records Notice (SORN) DOT/FAA 815 *Investigative Records System* 87 FR 51482 (August 22, 2022). Login credentials, audit trails, and security monitoring for FAA employees and contractors are handled in accordance with SORN DOT/ALL 13 *Internet/Intranet Activity and Access Records* 67 FR 30757 (May 7, 2002). The collection and maintenance of emergency contact information is handled in accordance with SORN DOT/ALL 22 *Emergency Contact Records Not Covered by Notices of Other Agencies* 75 FR 68852 (November 9, 2010). The management of general personnel records are handled in accordance with SORN OPM Govt. 1 *General Personnel Records* 88 FR 56058 (August 17, 2023).

Finally, the publication of this PIA further demonstrates DOT's commitment to provide

DOT Privacy Office - Approved - 10/22/2026

appropriate transparency into ITS.

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 with reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

PII is collected directly from individuals and thus is assumed to be accurate. Individuals seeking employment or an aviation certificate from the FAA agree to provide the necessary information to process their request, which includes name, SSN, driver's license number, and employment history. Anyone supplying their PII is presented with a PAS, for which the individual must acknowledge before providing their PII. Additionally, the individual completes the form themselves and thus verifies that all the data elements are correct.

PII is also received from data exchanges with ITS, where PII is sent electronically and not collected from the individual. These data exchanges are covered with PII Sharing Agreements and/or Memorandums of Understanding (MOU), which are reviewed every three years. These data exchanges with ITS include DOT Delphi Financial Management System (Delphi), DCSA eDelivery/Connect Direct System (eDelivery), FAA Identity Management System (IDMS), DOT Interface Repository (IR), Transportation Security Administration (TSA) Pre-Check system, DOT National Driver Register (NDR), MedExpress, a subsystem of the FAA Medical Support System (MSS), FAA Comprehensive Airmen Information System (CAIS), a subsystem of Civil Aviation Registry Applications (AVS Registry), FAA Enterprise Architecture and Solutions Environment (EASE), FAA Enforcement Information System (EIS), FAA Wisdom Insider Threat Identification (Wisdom ITI), and the FAA Automated Vacancy Information Access Tool for Online Referral (AVIATOR).

Individuals interested in challenging or questioning data items from other systems may contact the source system/agency for corrections as discussed in those systems' Privacy Impact Assessments (PIA) located at URL https://www.transportation.gov/individuals/privacy/privacy-impact-assessments.

Under the provisions of the Privacy Act, individuals may request searches of the ITS to determine whether any records have been added that may pertain to them and whether those records are accurate. For all inquiries related to the information contained in the ITS, the individual may appear in person, send a request via email (privacy@faa.gov), or in writing to:

Office of the Assistant Administrator for Security and Intelligence,
800 Independence Avenue, SW
Room 300
Washington, DC 20591

DOT Privacy Office - Approved - 10/22/2026

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

Individuals may also use the above address to register a complaint or ask a question regarding FAA's privacy practices. If individuals have comments, concerns, or need more information on FAA privacy practices, please contact the Privacy Division at privacy@faa.gov or 1 (888) PRI-VAC1.

Purpose Specification

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

ASH collects PII from individuals who wish to be employed by the FAA, either as employees or contractors. ITS processes background investigations under the following authorities:

- Title 49 United States Code (U.S.C.), chapter 449, *Air Transportation Security*, enacted as Pub. L. 103–272 on July 5, 1994. This authority legally mandates the system's collection of identity, credentialing, investigative, and enforcement records necessary to secure commercial air transportation, investigate aviation incidents, and enforce hazardous materials safety regulations.
- *The Transportation Safety Act of 1974*: This authority legally justifies the collection, maintenance, and processing of investigative, enforcement, and safety-related PII necessary to analyze aviation accidents, enforce hazardous materials compliance, and mitigate risks to air transportation.
- *FAA Drug Enforcement Assistance Act of 1988*: This authority provides for the collection of legally mandated records to combat illegal drug trafficking in aviation for ITS to process airmen registries, aircraft data, or drug-testing results.
- Executive Order (EO)10450 (*Security Requirements for Government Employment*): This authority sets forth why ITS must collect and store standard background check data, SF-85/SF-86 forms, and personal references for regular federal employees and contractors.
- EO 12968 (*Access to Classified Information*): This authority ITS processes deep security clearance data, polygraph results, or foreign contact logs for individuals requiring access to secret or top-secret intelligence.

DOT Privacy Office - Approved - 10/22/2026

- EO 12829 (*National Industrial Security Program*): This authority is used so that ITS can process security clearances, facility access logs, and PII belonging to private sector aerospace contractors or third-party vendor employees.

  The following PII is collected, used, and maintained in ITS for the following specific purposes:

- Personnel Security collects PII, including full name, SSN, DOB, city, state and country of birth, from job applicants, from FAA employees, and non-employees, which is used to process and track a wide range of personnel security investigations. These investigations include current employees as well as those of job applicants, contract employees, and any other individuals with access to FAA facilities, systems, or information.
- Internal FAA investigations use the information collected by personnel security from FAA employees and contractors and non-employees, including name, SSN, and DOB, to investigate the following types of allegations: alleged employee misconduct, falsification of official documents, security violations, or claims against the FAA, property theft, and other investigative services.
- LEAP Agents collect PII, including name, SSN, and DOB, from pilots/airmen and other FAA certificate holders, which is used to track investigations involving criminal activity. This information is used by the FAA and other investigative services to process suspects involved in criminal activity involving aircraft.
- ITS collects all related documentation and information associated with a DUI, DWI, or other drug offenses involving an FAA-registered pilot. PII includes name, DOB, address, driver's license number, airline certificate number, phone number, and case-related court documents, which are used to investigate the offense.

ITS uses this information in accordance with the purposes for which it is collected under the following SORNs:

- DOT/FAA 815 *Investigative Records System* 65 FR 19520 (August 22, 2022) in order that the FAA may conduct its investigations and personnel security programs in an efficient manner and document official actions taken based on information contained in these records.
- DOT/ALL 22 *Emergency Contact Records Not Covered by Notices of Other Agencies* 75 FR 68852 (November 9, 2010) covers emergency contact records about FAA employees/contractors and members of the public where the FAA needs to contact the individuals' emergency contact.
- OPM Govt. 1 *General Personnel Records* 88 FR 56058 (August 17, 2023)

DOT Privacy Office Approved - 10/22/2026

covers records about current or former FAA employees/contractors and is the official repository of the records, reports of personnel actions, and the documentation required in connection with these actions affected during the individual's Federal service.

- DOT/ALL 13 *Internet/Intranet Activity and Access Records* 67 FR 30757 (May 7, 2002) to provide information to any person(s) authorized to assist in an approved investigation of improper access or usage of DOT computer systems.

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.

ITS collects the minimum information necessary for the FAA's Personnel Security Program and Investigation Programs to process personnel security investigations, investigate employee misconduct and criminal activity by airmen and other certificate holders, and process civil/tort, administrative, and regulatory investigations against the FAA. SSNs are collected and utilized to positively identify individuals across the various components of the FAA and to verify the accuracy of the information received from data exchanges.

FAA retains PII for only as long as is necessary to fulfill the specified purpose(s) and in accordance with National Archives and Records Administration (NARA) approved records disposition schedules (GRS). NARA *Comprehensive Records Schedule* NC1-237-77-03 Item 6: *Official Investigative Case File Records*; Item 7: *Investigative Correspondence File Records* should be destroyed five years after destruction of the related file material; Item 8: *Investigative Index File Records;* Item 33: *Air Carrier Operations File Records* are permanent and should be transferred to the Federal Records Center four years after close of file or sooner if inactive. Offer to NARA 5 years after.

Information Systems Security records under NARA GRS 3.2, Item 31 should be destroyed 6 years after password is altered or user account is terminated. *User Profiles, Login Files, Audit Trail Files, and System Usage File Records* are deleted when no longer needed.

Information Access and Protection Records under NARA GRS 4.2, Item 120, *Classified Information Nondisclosure Agreement Records* are copies of nondisclosure agreements, such as SF 312, Classified Information Nondisclosure Agreement, signed by civilian and military personnel with access to information that is classified under standards put forth by executive orders governing security classification. For these records apply the disposition for the official personnel folder. *Intermediary Records* under NARA GRS 5.2, Item 20 are temporary and should be destroyed upon creation or update of the final record, or when no longer needed for business use, whichever is later. *Employee Emergency Contact Records* under NARA GRS 5.3, Item 20 should be destroyed when superseded or obsolete, or upon separation or transfer of employee.

DOT Privacy Office - Approved - 10/22/2026

Aviation Company Investigations and Inspections Not Referred for Legal Enforcement Action Records are covered by schedule DAA-0237-2022-0018-002 and should be destroyed 10 years after cutoff. *Investigative Case Files of Drug and Alcohol Violations by Individuals Forwarded to the Federal Air Surgeon Records* under DAA-0237-2018-0003 should be cutoff after receipt of expunction notice and then destroy case file 30 days after cutoff. *Security Programs Correspondence and Investigations records* under NC-237-75-001 Item 2A are permanent and are to be offered to National Archives 30 years after case is closed. *Administrative claims by or against the United States Records* under NARA GRS 1.1, Item 80 are temporary and should be destroyed 7 years after final action, but longer retention is authorized if required for business use.

Personal Identification Credentials and Card Records under NARA GRS 5.6 Item 120 are temporary and should be destroyed 6 years after the end of an employee or contractor's tenure, but longer retention is authorized if required for business use; *Personnel Security Investigative Report Records* under Item 170 and 171 are destroyed in accordance with delegated authority agreement or memorandum of understanding; *Personnel Suitability and Eligibility Investigative Reports* under Item 170 should be destroyed in accordance with the investigating agency instruction; *Reports and Records Created by Agencies Conducting Investigations Under Delegated Investigative Authority* Item 171 should be destroyed in accordance with delegated authority agreement or memorandum of understanding; *Personnel Security and Access Clearance Records* under Item 180 are temporary, should be destroyed 1 year after consideration of the candidate ends, but longer retention is authorized if required for business use; *Personnel Security and Access Clearance Records* under Item 181 are temporary and should be destroyed 5 years after employee or contractor relationship ends, but longer retention is authorized if required for business use; *Index to the Personnel Security Case File Records* under Item 190 should be destroyed when superseded or obsolete; and *Information Security Violations Records* case files about investigating alleged violations of executive orders, laws, or agency regulations on safeguarding national security information under Item 200 are temporary and should be destroyed 5 years after close of case or final action, whichever occurs sooner, but longer retention is authorized if required for business use.

DOT Privacy Office Approved: 10/22/2026

Use Limitation

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

FAA employs administrative and technical controls to limit the use of the information it collects and processes through ITS. All authorized users must review and adhere to the annual Rules of Behavior relating to ITS or access to files will not be granted. Additionally,

ITS has an audit and notification process to reduce the risk of user access to unauthorized files. The FAA limits the use of the PII in ITS to conduct investigations and personnel security programs and document official actions taken based on information contained in these records.

Records in ITS are maintained according to the following SORNs:

SORN DOT/FAA 815 *Investigative Record System* 87 FR 51482 (August 22, 2022) in order that the FAA may conduct its investigations and personnel security programs in an efficient manner and document official actions taken based on information contained in these records.

SORN DOT/ALL 22 *Emergency Contact Records Not Covered by Notices of Other Agencies* 75 FR 68852 (November 9, 2010) data used for one strict reason-notifying designated third parties in the event of an individual emergency.

SORN OPM Govt. 1 *General Personnel Records* 88 FR 56058 (August 17, 2023) to establish the legal authority, data boundaries, sharing rules, and retention schedules required to protect federal employee records within ITS.

In addition to other disclosures generally permitted under 5 U.S.C. §552(a)(b) of the Privacy Act, all or a portion of the records or information contained in the system may be disclosed outside DOT as a routine use pursuant to 5 U.S.C § 552a(b)(3) as follows:

System Specific Routine Uses:

- FAA provides to authorized representatives of United States air carriers the results of investigations of an individual that contain information related to aviation safety.

Departmental Routine Uses:

- In the event that a system of records maintained by DOT to carry out its functions indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular program pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the appropriate agency, whether Federal, State, local or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation, or order issued pursuant thereto.
- A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local agency maintaining civil, criminal, or other relevant enforcement information or other pertinent information, such as current licenses, if necessary to obtain information relevant to a DOT decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant or other benefit.

DOT Privacy Office - Approved 10/2_/2025

Access, authentication, and audit log records are maintained in accordance with SORN DOT/ALL 13 *Internet/Intranet Activity and Access Records* 67 FR 30757 (May 7, 2002).

In addition to other disclosures generally permitted under 5 U.S.C. §552(a)(b) of the Privacy Act, all or a portion of the records or information contained in the system may be disclosed outside DOT as a routine use pursuant to 5 U.S.C § 552a(b)(3) as follows:

- To provide information to any person(s) authorized to assist in an approved investigation of improper access or usage of DOT computer systems.

The Department has also published 15 additional routine uses applicable to all DOT Privacy Act system of records. SORN DOT/ALL 13 lists these additional routine uses in the "Department General Routine Use" section.

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 the information through electronic forms, manual data entry, and by system-to-system data exchanges. When PII is collected directly from the individual, the individual, or their representative, is responsible for ensuring the accuracy of the information being provided. Information collected in the DOT digital Form 1681, *Identification Card/Credential Application*, which is used when requesting an identification badge, and the SF 86 or SF 85, are filled out by the individual and thus assumed to be accurate.

When manually entering PII into ITS, PII integrity checks are conducted electronically. For example, fields contain restrictions such as not allowing alpha characters where numerical entries are required and where DOB is required, no future dates are permitted.

When the PII is received through system-to-system data exchanges, the FAA protects the integrity of the information in ITS by limiting access to authorized FAA personnel whose official duties require them to access and use the information. Additionally, the applications have automatic programmatic checks that prevent records with duplicate SSNs from being stored within the system. Also, audit logs are maintained and periodically reviewed.

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

DOT Privacy Office - Approved 10/22/2026

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 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 ITS to test security processes, procedures, and practices. The system operates on security guidelines and standards established by the NIST, and the ITS system owner restricts access to the records in ITS to only FAA personnel with a need to know. In accordance with FAA policy, all data in-transit and at-rest is encrypted, and access to electronic records is access-controlled and limited according to job function. Additionally, FAA conducts annual cybersecurity assessments to test and validate security process, procedures, and posture of the system.

System audit logs are reviewed to monitor for unauthorized use.

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.

The DOT/FAA 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. Access to ITS PII is limited according to job function.

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

DOT Privacy Office - Approved - 10/22/2026

Responsible Official

Atul Celly
System Owner
Manager, AXM-400 Business Services and Security Solutions

Approval and Signature

Karyn Gorman
Chief Privacy Officer KARYN MARIE GORMAN Digitally signed by KARYN MARIE GORMAN Date: 2026.10.22 12:44:44 -04'00'
Office of the Chief Information Officer

DOT Privacy Office - Approved - 10/22/2026