U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration (FAA)
Office of Security and Hazardous Materials Safety (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 Office of Security and Hazardous Materials Safety (ASH) processes background investigations under the authority of 5 Code of Federal Regulations (C.F.R.) 731.104(a), which requires that government employees and contractors undergo a background investigation to establish their suitability for federal employment. Additionally, in section 347 of the 1996 DOT Appropriations Act [codified at 49 United States Code (U.S.C.) § 40122(g)], Congress directed the FAA to develop and implement a new personnel management system that addresses the unique demands on the agency's workforce. 49 U.S.C. § 106(f)(2), provides that the FAA is the final authority for carrying out all functions, powers, and duties of the agency relating to the appointment and employment of all officers and employees of the FAA (other than Presidential and political appointees). Pursuant to the FAA's appointment and employment authority, the FAA requires individuals seeking FAA employment to undergo an investigation to establish suitability/fitness for employment. Additionally, ASH is authorized under 49 U.S.C. § 40113, to perform the investigative, operational, regulatory, and/or administrative assignments.

The FAA is publishing this Privacy Impact Assessment (PIA) 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.

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 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

ASH is responsible for the FAA Investigation Programs and the Personnel Security Program, which in turn, is responsible for processing suitability background investigations for FAA employees, contractors, pilots, aircraft owners, aircraft mechanics, job applicants, and non-employees needing access to FAA facilities. The Investigation Programs also involve 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 Investigations Tracking System (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.

[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).

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 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 Personnel Security (AXP) Personnel Security Specialist (PSS) then enter 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 requirement.

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 agency uses NEAP to initiate a personnel security background investigation request for non-employees. The non-employee fills out one of the above applicable forms for their job type. The sponsor logs into NEAP and manually enters the PII, which is stored and maintained in ITS.
- **Contractor Personnel** -Vendor Access Portal[4] (VAP) – Contractor companies that have a contract with the FAA use VAP to initiate a personnel security background investigation request. The new FAA contractor fills out one of the above applicable forms for their job type. VAP is then used to upload the contractors 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:

[2] Members of the public include potential FAA and contract employees, non-employees, airmen, other FAA certificate holders, and law enforcement.
[3] NEAP is a subsystem within ITS.

- 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
- 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 (eQIP) system, which provides fingerprints and submission of other applicable forms back to the AXP PSS. Note: eQIP is an OPM-managed system that is not FAA-controlled or managed.

Step 3 – Interim Decision (applies only to applicants/employees moving to a new position) 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 Department of Defense (DoD) Defense Counterintelligence and Security Agency

(DCSA) conducts the actual background investigation, where the data is uploaded by the AXP PSS to the DoD, DCSA, and OPM eQIP systems. The investigation process includes record searches, employment and education verifications, reference checks, and file reviews. Depending on the investigation type, 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 completion of the applicant/employee background investigation by DCSA, which is then transmitted to the FAA via a data exchange with the OPM eDelivery/Connect Direct System (eDelivery), AXP reviews the background investigation and adjudicates it. The 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.

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 FAA's personnel and security investigative efforts and to record the investigation outcome.

Internal Investigations

The second type of investigations within 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 relative to conduct and discipline matters. All internal investigations are handled in the Busser Investigation Management System (BIMS), a subsystem within ITS.

Internal Investigation Business Process:

Step 1 – National Case Intake Portal[5] (NCIP) Submission
An internal investigation begins when a manager logs into the NCIP, fills out a request,[6] and reports alleged employee misconduct, which is maintained in BIMS. The electronic

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

submissions allow 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 the 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 Department of Transportation (DOT) orders.

Step 6 – Investigation Offices

Investigations are conducted by the Office of Investigation (AXI-100), Investigations Standards and Policy Division (AXI-200); Advanced Threat Analysis and Mitigation Division (AXI-300); and Technical Investigations Division (AXI-400). 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 requestor, which contains a summary of the investigation findings.

Regulatory Investigations

The third type of investigations 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 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 investigations by these entities 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 include individual's (subject, witness, airman, etc.) name, DOB, address, company name, and aircraft owner details.
- Laser /UAS Events. This module tracks and coordinates Laser and UAS incident investigations. A Common Separated Variables (CSV) file is sent from ASH AXE-100 in an email and manually uploaded into ITS. The CSV file contains longitude, latitude, airport name, law enforcement, etc. When the file comes to ITS, it usually does not contain PII; however, it could contain the UAS registration information.

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 Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations[7].

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.

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 ITS, that 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 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 Standard Form (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 is handled in accordance with the Department's published System of Records Notice (SORN) DOT/FAA 815, *Investigative Records System,* 65 FR 19520 (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).

Finally, the publication of this PIA further demonstrates DOT's commitment to provide 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 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 Privacy Act Statement (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 include DOT Delphi Financial Management System (Delphi), OPM eDelivery/Connect Direct System (eDelivery), Identity Management System (IDMS), 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 system's Privacy Impact Assessments (PIA). All DOT and FAA systems PIAs are found at 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 if any records have been added that may pertain to them and if such 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 Hazardous Materials Safety

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

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

Purpose Specification

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

The Office of Security and Hazardous Materials Safety (ASH) collects PII from individuals who desire to be employed by the FAA, either as an employee or a contractor. The information, noted in this PIA Overview section above, is used to process background investigations under the authority of 5 C.F.R. 731.104(a), which requires government employees and contractors to undergo a background investigation to establish their suitability for federal employment. Additionally, in section 347 of the 1996 DOT Appropriations Act (codified at 49 U.S.C. § 40122(g), Congress directed the FAA to develop and implement a new personnel management system that addresses the unique demands on the agency's workforce. 49 U.S.C. § 106(f)(2), provides that the FAA is the final authority for carrying out all functions, powers, and duties of the agency relating to the appointment and employment of all officers and employees of the FAA (other than Presidential and political appointees).

ASH is authorized in the name of the FAA Administrator, in accordance with 49 U.S.C. § 40113, to perform the investigative, operational, regulatory, and/or administrative assignments required to accomplish the FAA mission, including the investigation of DUI/DWI infractions committed by anyone who possesses an Airman Certificate. This PII is processed in RITS

FAA/ASH collects and processes PII to facilitate the FAA's personnel security programs as well as to carry out the FAA's mission to promote civil aviation safety. The PII collected by ITS allows the FAA to conduct investigations and personnel security programs in an efficient manner and document official actions taken based on information contained in these records. These records are shared with BIMS when an internal investigation is initiated.

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 Agent's 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 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 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 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.

Social Security Numbers (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 the following National Archives and Records Administration (NARA) approved records disposition schedules:

- *Investigative Records* are maintained in accordance with NARA Schedule DAA-0446-2019-004 *Background Investigation Records External Relations Records*. Records are destroyed 5 years after an individual leaves the FAA unless there is pending legal or administrative action.

- *User Profiles, Login Files, Audit Trail Files, and System Usage File Records* are maintained in accordance with NARA General Records Schedule (GRS) 3.2: *Information Systems Security Records*. Item 31. Records are destroyed when no longer needed.

- *Classified Information Nondisclosure Agreement Records* are maintained in accordance with NARA GRS 4.2: *Information Access and Protection*, Item 120. Records are destroyed when 50 years old.

- The following records are maintained in accordance with NARA GRS 5.6: *Security Records:*

    - Item 120. *Personal Identification Credentials and Card Records* are destroyed 6 years after terminating an employee or contractor's employment, but longer retention is authorized if required for business use.

    - Item 170 and 171. *Personnel Security Investigative Report Records* are destroyed in accordance with delegated authority agreement or memorandum of understanding.

    - Item 180 and 181. *Personnel Security and Access Clearance Records* are destroyed 5 years after employee or contractor relationship ends, but longer retention is authorized if required for business use.

- Item 190. *Lists or Reports showing the current security clearance status of individual records* are destroyed 5 years after employee or contractor relationship ends, but longer retention is authorized if required for business use.

- Item 200. *Information Security Violations Records* are destroyed 5 years after employee or contractor relationship ends, but longer retention is authorized if required for business use.

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 process 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 on the basis of information contained in these records as detailed in SORN DOT/FAA 815, *Investigative Records System,* 65 FR 19520 (August 22, 2022). 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.

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 17 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."

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 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 to be 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 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*."

Responsible Official

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

Prepared by: Barbara Stance, FAA Chief Privacy Officer

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer