U.S. Department of Transportation

# Privacy Impact Assessment
# Federal Aviation Administration (FAA)
# Security & Hazardous Materials Safety (ASH)
# Internal Web Portal (IWP)


## Responsible Official

Atul Celly
Email: atul.celly@faa.gov
Phone Number: (202) 267-5662

## Reviewing Official

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


## Executive Summary

The Federal Aviation Administration (FAA) Security & Hazardous Material Safety (ASH) Internal Web Portal (IWP) serves as an information portal and subsystem launching page. It provides single sign on functionality for ASH employees and contractors to access ASH-managed subsystems within the internal FAA network. The ASH IWP operates under the following authorities: 49 United States Code (U.S.C.) chapter 449, *Security Transportation Safety Act of 1974*, the *FAA Drug Enforcement Assistance Act of 1988*, Executive Order (E.O.) 10450, *Security Requirements for Government Employment*, and E.O. 12968, *Access to Classified Information.*

The FAA is publishing this Privacy Impact Assessment (PIA) for ASH IWP 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 Foreign Nationals seeking approval to visit FAA facilities and potential FAA employees. The system also maintains PII for access and authentication from FAA employees and contractors including FAA employees/contractors being investigated by the FAA.

## 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 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:*



[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).

- *Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk, and of options available for mitigating that risk;*
- *Accountability for privacy issues;*
- *Analyzing both technical and legal compliance with applicable privacy law and regulations, as well as accepted privacy policy; and*
- *Providing documentation on the flow of personal information and information requirements within DOT systems.*

*Upon reviewing the PIA, you should have a broad understanding of the risks and potential effects associated with the Department activities, processes, and systems described and approaches taken to mitigate any potential privacy risks.*

## Introduction & System Overview

The Federal Aviation Administration (FAA) Security & Hazardous Materials (ASH) Internal Web Portal (IWP) serves as an information portal and subsystem launching page. ASH IWP operates under 49 United States Code (U.S.C.) chapter 449, *Security Transportation Safety Act of 1974*, the *FAA Drug Enforcement Assistance Act of 1988*, Executive Order (E.O.) 10450, *Security Requirements for Government Employment*, and E.O. 12968, *Access to Classified Information.*

ASH IWP was created so that FAA employees/contractors could quickly reach and be easily authenticated to all the subsystems/applications that are needed to conduct ASH business. Previously there were multiple websites and portals for authentication and access. ASH IWP streamlined this issue. ASH IWP serves as launching page for accessing FAA and ASH-managed systems. It provides single sign-on functionality for ASH employees/contractors to access ASH-managed subsystems within the internal FAA network. ASH IWP is only accessed by FAA employees and contractors. The international visitor's component of the ASH IWP request is initiated by the FAA Sponsor (FAA designated rep who collects all the information from the travelers for vetting and processing) who submits the foreign visitors' information and any requests to modify or update information is done by the FAA Sponsor. ASH IWP is hosted within the FAA Cloud Services Amazon Web Services EastWest environment. Each of the ASH subsystems that ASH IWP provides access and authentication to manages its own access authorization, data encryption, and privacy documentation in compliance with applicable requirements.

To use any of the below applications, authorized users gain access by using their Personal Identity Verification (PIV) card to login via MyAccess. Once logged in, the user can access and conduct transactions within each authorized subsystem.
The subsystems listed directly below only use ASH IWP single sign-on functionality as a launching point, but they all have separate security boundaries and privacy documentation, including PIAs. These subsystems are beyond the scope of this PIA:

- FAA Investigations Tracking System (ITS) – This application is used to conduct Security Background Investigations for FAA employees and contractors.

    - Transportation Safety Administration Pre-Check (TSA PreCheck) – This application is used for FAA Employees with a Secret Clearance or higher to register for TSA PreCheck for domestic air travel.

    - Senior Executive Agent Directive Reporting Tool (SEAD3) – This application is used to track selected groups of employees who are planning foreign travel and includes the FAA employee name.

    - International Travel Security Program Dashboard (ITSP) –ITSP's mission is to protect the FAA and the National Airspace System (NAS) by preparing official international FAA travelers with timely and pertinent information concerning the risks they may encounter while abroad. This site is a repository of safety and security information for countries of the world allowing the FAA employee to research and assess the risks of travel. Each section contains information on terrorism, political violence, crime, health, environmental, and other risks as well as resources to provide a complete overview.

    - List Server Email – This application is used for subscribing/unsubscribing to the ITSP mailing list and for sending mass emails to subscribers and includes the FAA employee/contractor name, FAA email, and Government Furnished Equipment (GFE) mobile number.

    - International Travel Follow-up Questionnaire (ITFQ) - This subsystem is used to capture any security risks encountered by an FAA employee during an international visit. Records are retrieved by FAA employee name, email address, and response to questions. SORN coverage is GSA/GOVT-4.

    - International Travel Loaner Verification (ITLV) – The application is used by FAA employees to determine if approval is needed for the GFE that they carry on international travel and includes the FAA employee name, GFE Computer Name, GFE FAA Mobile Number, and FAA email. Records are retrieved by the ASH IWP administrators using FAA employee name, email, office, GFE type, and country of travel.

    - International Travel Preapproval Request (ITPAR) – This application is used for the National Security Programs & Incident Response (AXE) to pre-approve any International Travel request submitted by AXE employees and includes FAA employee name. Records are retrieved by the ASH IWP

administrators using FAA employee name, FAA email address, or supervisor FAA email address.

- Identity Management System (IDMS) – This application is used to process FAA employees and contractors for a PIV card.
    - Employee Contractor Verification System (ECVS) – This application is used at FAA Facility Security Check Points to verify if an employee or contractor that is not in possession of their PIV Card is still authorized to access the facility. Records are retrieved by the ASH IWP administrators using (employee/contractor lookup date and location).
- Credential Issuance – This application is used to issue authorized FAA employee Credentials to do their assigned agency duties, the authority which they operate under is listed on the credential. Records are retrieved by the ASH IWP administrators using (name, credential type, issue date, and expiration date).

The following ASH subsystems within the ASH IWP security boundary are covered by this PIA. These subsystems only contain FAA employee and contractor PII.

- Personnel Access Security System (PASS) (Main ASH IWP functionality) – This application is used for the creation and management of user accounts required for access to ASH IWP, ITS, IDMS, and all ASH subsystems. PASS contains information to authenticate the user and to determine whether the user has been authorized to access a particular application and includes username, office, job type, office location, branch, and email address, which is entered directly into the database by administrators. Records are retrieved by the ASH IWP administrators using name, email address, facility city and state.
- Facility Security Reports System (FSRS) – This application is used to capture, process, and report information related to FAA facilities, physical security assessments, comprehensive and supplemental inspections, communications security, classified/Sensitive Security (SSI), physical security incidents, Secure Terminal Equipment/Secure Telephone Unit III (STE/STU III), facility accreditation, quarterly reports, and inspector reports. Also, the system has the audit capability on the major modules like assessment, inspection, and facility. Incident reports containing the result of a facility inspection deficiencies such as broken windows, locks, improper locks, and security cameras, are submitted via an internal online form. Records are retrieved by the ASH IWP administrators using facility name, address, and facility security level.
- Facility Security Reports System 2 (FSRS2) – This application is a Risk Assessment Tool. The FSRS2 application for tracking Based on Evaluation (BOE), Exceptions, and Waivers is assigned to an FAA Facility. The system is used for an information

management subsystem that is designed to capture, process, and report information related to FAA facilities, physical security assessments, comprehensive and supplemental inspections, communications security (COMSEC), Classified National Security Information (CNSI), Controlled Unclassified Information (CUI) Sensitive Security (SSI), physical security incidents, STE/STU III (obsolete and incorporated into COMSEC above), facility and secure area accreditation, quarterly reports, and inspector reports. Also, the system has the audit capability on the major modules like assessment, inspection, and facility. Incident reports containing the result of a facility inspection deficiencies such as broken windows, locks, improper locks, and security cameras, are submitted via an internal online form. Records are retrieved by the ASH IWP administrators using facility address, findings, incident, inspection date, and type.

- Credentials Verification System (CVS) – This is an application used to verify that an FAA credential is active and valid while being presented for access to FAA-inspected facilities and airports for conducting safety and security inspections. Records are retrieved by the ASH IWP administrators using date, time, successful attempts, and failed attempts.

- Conference Room Polycom Scheduler – This application is used to book conference rooms throughout all ASH Offices. Records are retrieved by the ASH IWP administrators using FAA employee/contractor name, room reservation date and time.

- Leave Scheduler – This application is used to publish ASH employee's and contractors' daily status (teleworking, leave, travel, or training) and includes the FAA employee name and status. Records are retrieved by the ASH IWP administrators using FAA employee name and work or non-work status.

- Executive Calendar – This application is used to publish ASH executive staff's daily status (teleworking, leave, travel, or training) and includes the FAA employee name and status. Records are retrieved by the ASH IWP administrators using FAA employee name and work or non-work status.

- Controlled Unclassified Information Destruction (CUI) Bin Application – This application is used to request, service, and inventory a CUI Bin (dumpster). The equipment is tracked by serial number, location, and FAA employee. Records are retrieved by the ASH IWP administrators using BIN serial number, location, bin type, and size.

- Vehicle Scheduler – This application is used to reserve government vehicles at various ASH offices that maintain a fleet of vehicles and includes the FAA employee name. Records are retrieved by the ASH IWP administrators using vehicle year, type, location, reservation date, and time.

- Program Management Maturity Reporting Tool (PM3) – This application is used to track and report incremental process improvements in ASH program offices. Records are retrieved by the ASH IWP administrators using non-PII target goals.

- Out of Agency Training Request (OATR) – This application is used by ASH employees to submit training requests when requested training is not available within the FAA-offered training and includes the FAA employee name. Records are retrieved by the ASH IWP administrators using FAA employee name, email address, training facility address.

- Call for Training (CFT) – This application is used by ASH Managers to suggest training for their staff and includes the FAA employee name. Records are retrieved by the ASH IWP administrators using FAA employee name and suggested training.

- Staffing Dashboard (internal employees only) – This application is used to track the hiring process of ASH employees (checklist for various positions including candidate selections, interviews, vacancy announcement posted, etc.) and includes the FAA employee name. Records are retrieved by the ASH IWP administrators using FAA employee position title, program office, position type, and number of vacancies.

- SharePoint ASH Portal – This application is used as a storage and collaboration tool between ASH staff offices. It can contain any of the PII in the system. It also provides a link to other ASH applications.

- ASH Suggestion Box – This application is used to ask questions and make suggestions directly to the ASH Director and Deputy Director and includes the FAA employee name.

- Community Security (COMSEC) – This application is used for conducting COMSEC inspections and reports and includes the FAA employee name. Records are retrieved by the ASH IWP administrators using COMSEC location, inventory, facility address, and room number.

- Classified Unclassified Information CUI – This application is used to track classified equipment and conduct inspections to ensure compliance (checklist for requirements like security checkpoints compliance, signs posted, etc.). Records are retrieved by the ASH IWP administrators using facility address room number.

- Web Incident Reporting (WebBIRS) – This application is used to report incidents that occur on or near FAA facilities and includes the FAA employee/contractor's name. Only FAA employees/contractors have access to this site. Records are retrieved by the ASH IWP administrators using name, email address, and incident description text.

**The following subsystem is the only ASH IWP subsystem that contains members of the public information (international visitors/foreign nationals):**

- There are two access points to International Visitors Program (IVP) system (internal and external). Both access points are only accessible to Department of Transportation DOT/FAA employees/contractors using their PIV card to access. IVP is used to process data from international visitors (Foreign Nationals) seeking approval to visit FAA facilities. To initiate a request to visit an FAA facility, the FAA Sponsor logs into URL https://visitors.faa.gov and clicks on the link for "International Visitors Program." A screen appears and prompts for login credentials (using webmail ID and password). After the Sponsor successfully logs in, they see a welcome page and a side menu specifying options to initiate a request with or without POC.

    - If the Sponsor is working with a Visitor Coordinator (POC) to supply all visitor required information including address, date of birth (DOB), passport, employer, etc.) then "Visit Request (POC)" is selected. The Sponsor enters facility information, basic visitor information, and the contact's name and email of the Visitor Coordinator.

    - If the sponsor is entering this information directly without a visitor coordinator POC then "Visit Request (No POC)" is selected, and the Sponsor enters the facility and full visitor information.

  Using FAA Electronic Form SF-1600.78 Visitor Form, the following PII is entered: International visitor/foreign national name, address, country, gender, DOB, birth city, birth country, current citizenship, dual citizenship country, passport number, visa type, job title or position, name of employer, employer address, and employer country. Once the form is submitted to the FAA's Office of International Affairs (API) via the webform, the data is used by API to review the visit and forward it to AXM, ASH Service Area personnel, and the appropriate LOB for review. ASH Service Area personnel forward the visit request to the appropriate FAA facility manager for approval. This PII is stored in an encrypted database within the ASH program. Foreign Nationals records are retrieved by the ASH IWP administrators using name, country, Visit Request ID number, sponsor name, email, dates of visit, passport number, country, gender, and DOB.



## 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) 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.*

## 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.*

ASH IWP is a privacy-sensitive system because it maintains collects, uses, disseminates, and retains PII from FAA employees and contractors including Foreign Nationals for the purpose of vetting FAA facility visit requests. Policies, procedures and practices for information storage, data use, access, notification, and retention and disposal are described here in this PIA.

Records are retrieved using FAA employee/contractor name and FAA email address. Foreign Nationals records are retrieved by the ASH IWP administrators using name, country, Visit Request ID number, sponsor name, email, dates of visit, passport number, country, gender, and DOB. The FAA protects records subject to the Privacy Act in accordance with the following Department's published System of Records Notices (SORNs):

- DOT/ALL 9, *Identification Media Record Systems* 67 FR 62511 (October 7, 2002)[2], which covers FAA employee/contractor credentialling records and the following subsystems ECVS and Credential Issuance. Also, covers Foreign Nationals records within IVP.
- DOT/ALL 27, *Training Programs* 83 FR 60960 (November 27, 2018), which covers FAA employee training records, and the following subsystems OATR and CFT.
- OPM GOVT-1, *General Personnel Records* 88 FR 56059 (August 17, 2023), which covers FAA employees' records regarding the hiring process, and the

[2] DOT/ALL 9 is being updated.

following subsystems Staffing Dashboard, Leave Scheduler, and Executive Calendar.

- DOT/FAA 815 - Investigative Record System - 87 FR 51482 - August 22, 2022 which covers records for FAA employees and incidents that occur on or near FAA facilities and the WebBIRS subsystem.
- DOT/ALL 16, *Mailing Management Systems* 71 FR 35319 (June 19, 2006), which covers records for subscribing/unsubscribing to a mailing list and for sending mass emails to subscribers and the List Server Email subsystem.
- GSA/GOVT–4, *Contracted Travel Services Program* 74 FR 26700 (July 6, 2009) which covers records regarding FAA employee international travel and the SEAD3 subsystem.

The FAA uses access information for purposes of creating and validating login credentials, audit trails, and security monitoring for FAA employees and contractors who are part of the program and/or manage the system. This use is consistent with the description in the "purpose" section in the following SORN DOT/ALL 13, *Internet/Intranet Activity and Access Records* 67 FR 30757 (May 7, 2002).

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

Under the provisions of the Privacy Act, individuals may request searches of the ASH IWP system to determine if any records have been added that may pertain to them and if such records are accurate. Much of the data that flows through IWP is ultimately saved and maintained in other systems. Please refer to the applicable system's PIA covering those at URL https://www.transportation.gov/individuals/privacy/privacy-impact-assessments and follow the instructions contained in the PIA.

For all inquiries related to the information contained in the ASH IWP, 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.

## 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.*

Congress has authorized the FAA Administrator to develop systems and/or tools to support FAA business needs. ASH IWP addresses the unique demands of the FAA's workforce and operates under the following authorities:

49 U.S.C. chapter 449, *Security Transportation Safety Act of 1974*; the *FAA Drug Enforcement Assistance Act of 1988*; E.O. 10450, *Security Requirements for Government Employment*; E.O. 12968, *Access to Classified Information.*

ASH IWP collects PII for the following purposes:

- FAA facility visit requests
- System access
- Issuing credentials
- Training
- Monitoring the internal ASH employee hiring process
- Incident reporting
- International travel
- Subscribing/unsubscribing to ASH mailing list

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

- DOT/ALL 9, *Identification Media Record Systems* 67 FR 62511 (October 7, 2002), which covers FAA employee/contractor credentialling records and the following subsystems ECVS and Credential Issuance. Also, covers Foreign Nationals records within IVP.

- DOT/ALL 27, *Training Programs* 83 FR 60960 (November 27, 2018), which covers FAA employee training records, and the following subsystems OATR and CFT.
- OPM GOVT-1, *General Personnel Records* 88 FR 56059 (August 17, 2023), which covers FAA employees records regarding the hiring process, and the following subsystems Staffing Dashboard, Leave Scheduler, and Executive Calendar.
- DOT/FAA 815 - Investigative Record System - 87 FR 51482 - August 22, 2022, which covers records for FAA employees and incidents that occur on or near FAA facilities and the WebBIRS subsystem.
- DOT/ALL 16, *Mailing Management Systems* 71 FR 35319 (June 19, 2006), which covers records for subscribing/unsubscribing to mailing list and for sending mass emails to subscribers and the List Server Email subsystem.
- GSA/GOVT–4, *Contracted Travel Services Program* 74 FR 26700 (July 6, 2009) which covers records regarding FAA employee international travel and the SEAD3 subsystem.

Records created for the purposes of FAA employee/contractor user account creation, logging, auditing, etc. are covered by SORN DOT/ALL 13 *Internet/Intranet Activity and Access Records* 67 FR 30757 (May 2002).

## 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 information from individuals to support FAA's business needs. The FAA maintains different types of records in accordance with applicable National Archives and Record Administration (NARA) approved General Retention Schedules[3] (GRS). Please see Appendix A for the full listing of record schedules that cover the records in ASH IWP. The system owner restricts access to the records in ASH IWP 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.

User system access and audit log records are maintained in the system as temporary records and are destroyed when business use ceases. The applicable records retention

[3] 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 to promote consistent retention practices.

schedule is NARA GRS 3.2, *Information Systems Security Records*, Item 30, approved January 2023. DAA-GRS-2013-0006-0003.

## 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 employs administrative and technical controls to limit the use of the information it collects and process through ASH IWP. The ASH External Web Portals (EWP) system is an external facing website where FAA employees can initiate a request for Foreign Nationals/ international visitors to visit an FAA facility. The request is submitted to the ASH EWP and processed from IWP via a data transfer. The PII in ASH IWP is used for approved ASH business processes and access and authentication to the system. The FAA does not use the PII for any other purpose. All authorized users must review and adhere to the annual Rules of Behavior relating to ASH IWP or access will not be granted. Additionally, ASH IWP 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 ASH IWP to access and authentication and to conduct approved, authorized business.

FAA employee/contractor users that access applications from the ASH IWP get their authenticated variables passes through MyAccess which sends the authenticated users' data to the specific application for access authorization, which is managed and controlled at each application level. The (PII) Sharing Agreement between AIT MyAccess and ASH IWP covers this data exchange.

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

- DOT/ALL 9, *Identification Media Record Systems* 67 FR 62511 (October 7, 2002), which covers FAA employee/contractor credentialling records and the following subsystems ECVS and Credential Issuance. Also, covers Foreign Nationals records within IVP.
- DOT/ALL 27, *Training Programs* 83 FR 60960 (November 27, 2018), which covers FAA employee training records, and the following subsystems OATR and CFT.
- OPM GOVT-1, *General Personnel Records* 88 FR 56059 (August 17, 2023), which covers FAA employees records regarding the hiring process, and the

following subsystems Staffing Dashboard, Leave Scheduler, and Executive Calendar.

- DOT/FAA 815 - Investigative Record System - 87 FR 51482 - August 22, 2022, which covers records for FAA employees and incidents that occur on or near FAA facilities and the WebBIRS subsystem.
- DOT/ALL 16, *Mailing Management Systems* 71 FR 35319 (June 19, 2006), which covers records for subscribing/unsubscribing to mailing list and for sending mass emails to subscribers and the List Server Email subsystem.
- GSA/GOVT–4, *Contracted Travel Services Program* 74 FR 26700 (July 6, 2009) which covers records regarding FAA employee international travel and the SEAD3 subsystem.

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).

Other disclosures are permitted under 5 U.S.C. §552(a)(b) of the Privacy Act.
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, and 77 FR 42796, July 20, 2012, 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. Because PII is collected directly from the individual, the individual or their representative is responsible for ensuring the accuracy of the information being provided. ASH IWP collects, uses, and retains data that is relevant and necessary for the purpose for which it was collected.

ASH IWP has procedures and processes in place to ensure that once the program receives the information, it is as accurate, relevant, timely, and complete as possible. The FAA protects the integrity of the information in ASH IWP 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 duplicative records to be stored within the system. Also, audit logs are maintained and periodically reviewed.

PII integrity checks are conducted electronically, for example, fields containing restrictions such as only allowing alpha characters and future dates for DOB are not permitted.

## 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 ASH IWP to test security processes, procedures, and practices. The system operates on security guidelines and standards established by the NIST, and the ASH IWP system owner restricts access to the records in ASH IWP 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 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 ASH IWP 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 ASH IWP 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

## Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN MARIE GORMAN
Digitally signed by KARYN MARIE GORMAN
Date: 2024.10.08 09:04:58 -04'00'