U.S. Department of Transportation

Privacy Impact Assessment
Federal Aviation Administration (FAA)
Security and Hazardous Materials Safety (ASH)
External Web Portal (EWP)

Responsible Official

Atul Celly
Manager, Business Services and Security Solutions Division, AXM-400
202-267-4930
9-AWA-ASH-APPSupport@faa.gov

Reviewing Official

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

Executive Summary

The Federal Aviation Administration (FAA) Office of the Assistant Administrator for Security and Hazardous Materials (ASH) External Web Portal (EWP) is used as a pass-through portal that facilitates multiple ASH business processes for individuals that do not have a Personal Identity Verification (PIV) card and need various FAA services. EWP is also used to transfer the data to internal FAA systems and databases. EWP 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.*

This is an update to the previously published EWP Privacy Impact Assessment (PIA) to reflect changes made to the system since its original publication. The FAA is publishing this PIA for the EWP pursuant to Section 208 of the E-Government Act of 2002 because EWP collects and processes Personally Identifiable Information (PII) from members of the public (potential FAA contractors, airman certificate holders,[1] military personnel, federal/state agency employees, and those that do not have a PIV card).

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.[2]

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

[1] These airman certificate holders include private, commercial, and airline transport pilots.

[2] Office of Management and Budget's (OMB) definition of the PIA is taken from guidance on implementing the privacy provisions of the E-Government Act of 2002 (see OMB memo of M-03-22 dated September 26, 2003).

electronic information systems and collections handle personally identifiable information (PII). The goals accomplished in completing a PIA include:

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

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

Introduction & System Overview

The Office of Security Hazardous Materials Safety (ASH) is responsible for processing background investigations for FAA potential contractors. ASH is also responsible for providing security awareness training for FAA contractors who support the FAA and do not possess an FAA-issued PIV Card. EWP also provides a website for Airman Certificate holders/pilots to submit notifications of an arrest involving drugs and or alcohol-related incidents. EWP was established to simplify these business processes and is the launching point for collection and submission of PII.

ASH EWP is a pass-through portal that facilitates ASH business processes via nine applications (fully detailed below) for members of the public (potential FAA contractors, airman certificate holders, military personnel, federal/state agency employees, and those that do not have a PIV card), but that need various FAA services. Once collected, the data is transferred to other internal FAA ASH systems/repositories, where it is stored/maintained. When the member of the public submits their PII, it is immediately encrypted, transferred to the subsequent system/program, and then immediately deleted from the EWP. The only PII maintained in ASH EWP is access and authentication information (username/email and password).

The EWP is a collection of the following subsystems/services:

Vendor Access Portal (VAP) – VAP enables the FAA contracting company's point of contact (POC) to submit online applications for their new, potential FAA contractor employees to initiate the FAA pre-employment investigation. The FAA contracting company POC is assigned a username and password and then accesses the VAP at a designated Uniform Resource Locator (URL). The POC provides the PII (about the potential FAA contractor/the contracting company's contractor employee to be investigated) in a set of web forms. The VAP is utilized to submit PII for potential FAA contractors including their first name, last name, suffix, date of birth (DOB), place of birth, country of birth, Social Security Number (SSN), and email address. The potential contractor does not have direct access to the system. The VAP uses a 2-factor authentication process to allow authorized users access only for submission. After the POC enters the data and hits submit, the file is auto encrypted and immediately transferred to the FAA ASH Investigations Tracking System (ITS) for processing (see ITS PIA[3]). The original data entered in the VAP database is immediately transferred and not maintained in VAP/EWP.

International Visitor Program (IVP) – The IVP is a web-based subsystem that processes data from international visitors seeking approval to visit FAA facilities using FAA Form 1600.78. On occasions when international visitors seek to visit FAA facilities, IVP sends an email to the FAA employee (sponsor) who is sponsoring the visit to the FAA. The email contains a secure link to the IVP website that permits temporary access to submit information. The visit sponsor accesses the IVP site and enters the PII of the individual who is seeking access to a FAA site into the online form 1600.78. The IVP subsystem receives the data and stores it temporarily in encrypted form in a database in EWP. The data is periodically transferred to the internal Web Portal (WP). The original data in the IVP database on EWP is then deleted. Once in the internal WP, the data is then used by ASH security personnel to review and decide on granting permission for the visit. The data is also reviewed by the FAA Service Security Elements on behalf of the appropriate FAA facility manager, by the FAA International Planning Office, and by the appropriate FAA Line of Business. Once this vetting process is complete, the international visitor seeking access is notified whether they are approved to access the FAA facility.

DUI/DWI Notification Letter Database – This database is used by active, certificated pilots to self-report an incident involving a drug and/or alcohol-related motor vehicle actions (MVA) to the agency's Security and Hazardous Materials Safety Office, Regulatory Investigations Division. Part 61 certificate holders are required to make notification of drug and/or alcohol related MVA to the FAA. The certificate holders navigate to URL https://ashapps.faa.gov/notificationletter and submit their email address to receive an email with a link to access the notification letter form. The form contains a valid Office of Management and Budget (OMB) Control Number, 2120-0543, for the collection of this information. Also, there is a Privacy Act Statement (PAS), which details the authority to collect their PII, the purpose and routine uses for their information, and what happens if the pilot fails to provide the requested PII. Once the pilot submits the required information via the link it instantly transfers all data to the FAA's ITS for processing, where it is maintained

[3] https://www.transportation.gov/sites/dot.gov/files/2023-10/Privacy%20-%20FAA%20-%20ITS%20-%20PIA%20-%202023.pdf

and stored and covered by separate ITS privacy documentation. When the pilot hits submit, the file is auto encrypted transferred to ITS, and deleted immediately from EWP. No data is maintained on the EWP.

Security Awareness Virtual Initiative (SAVI) Course – SAVI is a tool that ASH uses to train contractors and members of the public on security requirements, measures, and safeguards to protect FAA assets. This training course replicates the course that is offered through the FAA's Enterprise Learning Management System (eLMS); however, the difference is that this is offered on a public-facing website, so that FAA employees and contractors, who do not have access to the FAA intranet, can still take the training. Any member of the public that wants to take this training, may do so, by navigating to the URL and taking the course. The user registers for the training at URL https://ashsavi.faa.gov. The only information stored in EWP is the username and password, which is encrypted. When the individual provides the required information, the file is auto encrypted, transferred to the FAA ASH "Internal" Web Portal (WP) system, which has its privacy documentation, and then immediately deleted from EWP.

ASH Classified National Security Information (CNSI) Course – ASH developed this course, "*Safeguarding Classified Information within the FAA*," to meet the training requirements referenced in FAA Orders 1600.1E and 1600.2E. This training course replicates the course that is offered through the FAA's eLMS; the difference is that this is a public-facing website so that FAA employees and contractors including members of the public, who do not have access to the FAA intranet, can take the training. All FAA employees and contractors, and members of the public (military personnel, and federal and state agency employees) who do not have a PIV card, but who hold security clearances must receive training on the basic Safeguarding Classified Information principles and practices. Any member of the public that wants to take this training, may do so, by navigating to the URL and taking the course. The user registers for the course at URL https://ashcnsi.faa.gov. When the individual provides the required information, the file is auto encrypted, transferred to an internal FAA ASH database, and then immediately deleted from EWP. It is not stored in EWP.

Customer Service (CS) Survey – CS survey is a web form accessed from a hyperlink that is appended to all ASH employee email signatures. EWP uses this service to assess the ASH employees and contractors service that is provided to FAA customers. The results are maintained internally in the ASH program and only shared with the requesting FAA manager who reviews the feedback. When the reviewer submits their comments and/or PII, the file is auto encrypted, transferred internally to the ASH program and deleted immediately from EWP. These surveys can be filled out and submitted by members of the public that provide comments and their information (name, email, phone number) is optional if they request a response.

The FAA Insider Threat Program* and *Reacting to an Active Shooter Event Course – This is a course offered to familiarize FAA employees and contractors with the FAA Insider Threat and Active Shooter programs, which highlight if you "See Something, Say Something" and run, hide, fight. This training course replicates the course that is offered through the FAA eLMS; however, the difference is that it is a public-facing website so that anyone, who does not have access to the FAA intranet, can still take the training. Any member of the public that wants to take this training, may do so, by navigating to the URL and taking the course. The user registers at URL https://ashapps.faa.gov/astpublic. Information needed to create a profile to take the training is name, email address, username, password, and company name, if applicable. The information is collected, held temporarily in encrypted form, and then stored in an encrypted, internal ASH database. It is not stored in EWP. When the individual submits their information, the file is auto encrypted, transferred internally to the ASH program, and deleted immediately from EWP. The only information stored in EWP is the username and password, which is encrypted.

Policies, procedures, and practices for information storage, data use, access, notification, retention, and disposal are described herein in this PIA.

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template is based on the fair information practice principles (FIPPs). The FIPPs, rooted in the tenets of the Privacy Act, are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs provide a framework that will support DOT efforts to appropriately identify and mitigate privacy risk. The FIPPs-based analysis conducted by DOT is predicated on the privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v3, 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.

EWP is a privacy-sensitive system because it collects and disseminates PII, including the Social Security Number (SSN), from members of the public (potential FAA contractor employees) including from FAA contractors for background investigations. EWP also collects and disseminates PII from Commercial Pilots to ensure they are complying with Part 61 Certificate Holder Requirements. However, EWP is not a system of records subject to the Privacy Act (PA) because it is not designed to be searchable by name, address, phone number, or any other PII field. All PII collected through EWP, except the access and authentication data, is sent to other FAA systems and is not maintained by EWP.

Because EWP is the initial collection point for PII from potential FAA contractors and pilots reporting an alcohol-related conviction, the EWP provides a Privacy Act Statement (PAS) to these individuals to inform them how the FAA is using their PII. However, all other consent mechanisms are handled by the PA system of records that maintains the information, the FAA ASH Investigations Tracking System (ITS). See the ITS Privacy Impact Assessment (PIA) located here: https://www.transportation.gov/individuals/privacy/pia-investigative-tracking-system-its

The portal does not retrieve records by PII and thus no System of Records Notice (SORN) is required for EWP, except for SORN DOT/ALL 13, *Internet/Intranet Activity and Access Records*, 67 FR 30757 (May 7, 2002), which covers access and authentication records of all DOT employees, contractors, or other users authorized or unauthorized who access the Internet/Intranet through any of the authorized DOT network computers or mainframe/enterprise servers.

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

Potential FAA contractors applying for positions with the FAA can change data submitted through the VAP by submitting FAA Standard Form (SF)-85P with the correct information and contacting the Personnel Security Specialist handling their investigation in the FAA Security & Hazardous Materials- Investigations Program Office.

All PII that is collected through the EWP (except access and authentication data) is sent to the FAA ASH Investigations Tracking System (ITS). For redress and for an individual to update or edit their information that may be collected via EWP, the individual needs to follow the processes and procedures detailed in the ITS Privacy Impact Assessment (PIA) located here: https://www.transportation.gov/individuals/privacy/pia-investigative-tracking-system-its

If you have comments, or 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.

EWP operates under the following authorities:

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

PII collected via EWP includes members of the public (potential FAA contractors) full name, date of birth, personal/business email address, SSN, and citizenship status and is collected to for processing contractor background investigations. Additionally, PII collected in IVP includes members of the public and DOT federal/contract workforce full name, gender, place of birth, date of birth, and country or countries of citizenship, Passport and VISA information, and title, position, or description of visitor's duties and is collected to process security checks for international visitors entering FAA facilities. All data collected via EWP (except access and authentication data) is sent to the ITS

Finally, PII is also collected and maintained in EWP from FAA employees and contractors, and members of the public including name, username/email, password for access and authentication to FAA training programs and other FAA systems, which is covered by SORN DOT/ALL 13, *Internet/Intranet Activity and Access Records,* 67 FR 30757 (May 7, 2002) and used to manage access, authentication, and audit logs.

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 ASH programs. Because the individual provides the submitted information to their company, which is then submitted through EWP, the information is presumed to be accurate. Additionally, the system has an automatic business process in place where all data that is sent through the system (except access and authentication data) is deleted every 30 minutes.

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

- Information Technology Operations and Maintenance Records,[5] item 20, are records related to the activities associated with the operations and maintenance of the basic systems and services used to supply the agency and its staff with access to computers and data telecommunications. Includes the activities associated with IT equipment, IT systems, and storage media, IT system performance testing, asset and configuration management, change management, and maintenance on network infrastructure. The records are temporary and should be destroyed 3 years after the agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated, or superseded, but longer retention is authorized if required for business use.

- System Access Records,[6] item 30, are records created as part of the user identification and authorization process to gain access to systems. Records are used to monitor inappropriate system access by users. These records are temporary and should be destroyed when business use ceases.

Use Limitation

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

EWP serves as an entry point for submitting PII, including SSNs, to carry out various, approved FAA business processes. EWP limits the collection of PII to only the PII

[4] General retention schedules are used by the FAA to determine how long to maintain an individual's records and/or when to delete the individual's records order to promote consistent retention practices.

[5] NARA GRS 3.1, *General Technology Management Records*, January 2017. DAA-GRS-2013-00050004.

[6] NARA GRS 3.2, *Information Systems Security Records*, September 2016. DAA-GRS 2013-0006-0003.

necessary to conduct the required business processes. The FAA does not use the PII for any other purpose. The system does not retrieve records using a personal identifier. Access and authentication records within DTF are handled in accordance with SORN DOT/ALL 13, *Internet/Intranet Activity and Access Records*, 67 FR 30757 (May 7, 2002). 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 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."

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

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).

EWP only collects data that is relevant and necessary for the purpose for which it was collected. The potential contractor's PII is manually input by the FAA contractor company representative into EWP using the online input form. Once the data is transferred to the FAA Investigative Tracking System (ITS), the data is verified and cross-checked against the data submitted directly by the potential contractor on their SF-85P form. The FAA Personnel Security Specialist responsible for investigating the individual can determine if there are any inaccuracies in the data submitted in the VAP by contacting the potential FAA contractor directly. Because the PII is collected directly from the individual who is responsible for ensuring the correctness of the information provided, it is presumed to be accurate.

Additionally, PII integrity checks are conducted electronically when manually entering PII into EWP. For example, fields contain restrictions such as not allowing alpha characters where numerical entries are required and where date of birth is required, no future dates are 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, unauthorized access, destruction, usage, modification, and 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).

EWP takes appropriate security measures to safeguard PII and other sensitive data. For the VAP, the FAA contract company representative must first log into the VAP using a username and password provided by the FAA. All ASH Training applications within EWP (SAVI, CNSI, and Insider Threat) user information is encrypted and secured. Additionally, in all cases, the communication sessions are encrypted using Hypertext Transfer Protocol Secure (https), so that the PII data is protected during transmission. EWP is protected behind the FAA ENET firewalls as well as behind the firewall on the EWP subnet. The data is stored in encrypted form and is stored there only temporarily. Every 30 minutes all data, except access and authentication data, that has been submitted to EWP is transferred to the appropriate internal database within ASH and then the data is erased from EWP. In addition, EWP is also Personal Identity Verification (PIV) enabled.

Lastly, EWP has gone through a cybersecurity assessment and was issued a three-year Authorization to Operate (ATO). Further, EWP goes through an annual independent risk assessment to test security processes, procedures, and practices. The system operates on security guidelines and standards established by NIST and only FAA personnel with a need to know are authorized to access the records in EWP. The ATO is reviewed and updated based on the outcome of security testing and evaluation in accordance with FISMA. Access to EWP is limited to those with appropriate security credentials, an authorized purpose, and a need to know. The FAA deploys role-based access controls in addition to other protection measures reviewed and certified by the FAA's cybersecurity professionals to maintain the confidentiality, integrity, and availability requirements of the system.

Accountability and Auditing

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

FAA is responsible for identifying, training, and holding Agency personnel accountable for adhering to FAA privacy and security policies and regulations. FAA follows the Fair Information Principles as best practices for the protection of information associated with the EWP. The FAA Rules of Behavior (ROB) for IT systems governs EWP. The FAA's Office of the Chief Information Officer, Office of Information Systems Security, and Privacy Division are responsible for governance and administration of FAA Order 1370.121B, FAA *Information Security and Privacy Program & Policy*. Mandatory annual security and privacy training, as well as the FAA ROB, provides necessary guidance to the handling of data by EWP. The FAA ROB for IT Systems must be read, understood, and acknowledged by each user prior to a user's authorization to access the system. The FAA conducts regular periodic security and privacy compliance reviews consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), *Securing Agency Information Systems.*

Additionally, FAA has implemented 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.

Responsible Official

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

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN MARIE GORMAN

Digitally signed by KARYN MARIE GORMAN
Date: 2024.04.26 12:36:52 -04'00'