U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration (FAA)

Office of Information & Technology Services (AIT)

vFairs

Responsible Official

Veronica Bunn
Aviation Ecosystem Stakeholder Engagement Office
Office of the Chief Information Security Officer
ACI-Executive-Secretariat@faa.gov

Reviewing Official

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

Executive Summary

Pursuant to the Administrator's general authority under 49 United States Code 322, General Powers, and 49 United States Code 40101, Policy, the Federal Aviation Administration (FAA) purchased the vFairs software for use in performance of FAA activities. vFairs is a software used by the Office of Information & Technology Services (AIT) to host an informational website regarding the FAA's Cyber Rodeo events. Members of the public (employees of other federal agencies), FAA employees, and contractors access the website and use the virtual platform to sign up for aviation cyber events.

This Privacy Impact Assessment (PIA) is being performed pursuant to the E-Government Act of 2002 because vFairs collects sign-up information, including Personally Identifiable Information (PII) on members of the public, FAA employees, and contractors in order to process event registrations.

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:

- *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;*

[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).

- *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

vFairs is a software used by the Office of Information and Technology Services (AIT) to host an informational website regarding the Federal Aviation Administration's (FAA) Cyber Rodeo events. The vFairs software hosts the publicly accessible sign-up page (2022 ACI Cyber Rodeo (vfairs.com)) for the FAA's Cyber Rodeo events. Members of the public (employees of other federal agencies), FAA employees, and contractors access the website and sign up for electronic cyber events.

To sign up for an event, the individual must manually input the following: first name, last name, email address, organization/agency, phone number (optional), participant type (government employee/contractor), job title, participation in capture the flag (yes/no), attendance (virtual or in person), interest in table space (yes/no). Once the user submits their registration, an automated email is generated with a "save the date" and reservation confirmation. Users also have the opportunity to review the vFairs Privacy Policy.

The FAA accesses registration information via an Excel spreadsheet, which they download from vFairs. The FAA saves this information on an FAA SharePoint (Microsoft 365) site. The SharePoint site requires appropriate credentials to access this report and the report is protected and only accessible with a username and password. Registration data is not shared with outside vendors. Information present in the Excel spreadsheet is not retrievable by a unique identifier. Therefore, there no Privacy Act system of records is created through the use of vFairs.

Fair Information Practice Principles (FIPPs) Analysis

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

v3[2], sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council and the Privacy Controls articulated in Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations[3].

Transparency

Sections 522a(e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act require public notice of an organization's information practices and the privacy impact of government programs and activities. Accordingly, DOT is open and transparent about policies, procedures, and technologies that directly affect individuals and/or their personally identifiable information (PII). Additionally, the Department should not maintain any system of records the existence of which is not known to the public.

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. vFairs maintains a corporate Privacy Policy on its website that is accessible to all users to view. Users can review that policy before submitting their information to make an informed decision to provide information to the FAA using vFairs.

The publication of this PIA on the DOT Privacy website further demonstrates DOT's commitment to provide appropriate transparency regarding the handling of such information.

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.

Individuals are responsible for ensuring information they submit to FAA through vFairs is accurate. If an individual needs to update or make changes to their registration information, they can email the above-listed system owner who makes the required manual updates to the spreadsheet. Users can deactivate their accounts by emailing vFairs at tech@vfairs.com.

[2] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf
[3] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf

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.

vFairs collects, maintains, uses, or disseminates PII about members of the public, FAA employees, and contractors, pursuant to the Administrator's general authority under 49 United States Code 322, General Powers, and 49 United States Code 40101, Policy. Registration PII is maintained on members of the public, FAA employees, and contractors in order to allow individuals to sign up to attend cyber aviation events.

To sign up for an event, the individual must manually input the following: first name, last name, email address, organization/agency, phone number, participant type (government employee/contractor), job title, participation in "Capture the Flag" game (yes/no), attendance (virtual or in person), interest in table space (yes/no). This information is then provided via spreadsheet to the FAA. The FAA only uses this PII to plan and manage the Cyber Rodeo event.

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 and maintains only the minimum amount necessary for the FAA to plan and manage Cyber Rodeo events. vFairs saves the data only until the event is complete. The data may be used to create reports de-identified of PII for metrics purposes. Once reporting is complete, all registration data is deleted.

The system access records are retained and disposed of by the FAA in accordance with National Archives and Records Administration General Records Schedule 3.2, item 130, *Information Systems Security Records*. These records are destroyed when business use ceases. General Technology Management Records are maintained pursuant to General Records Schedule 3.1, items 011 and 020. Records maintained under item 011 are destroyed 5 years after being superseded by a new system. The spreadsheet maintained by the FAA is maintained in accordance with General Records Schedule 5.2, *Transitory and Intermediary Records*, item 10, and is destroyed when no longer needed 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.

Registration information collected on cyber rodeo registrants is maintained in an excel spreadsheet, and individual spreadsheets are not retrieved by unique identifier (although search functions of course exist within any particular excel spreadsheet, in the same manner as most other documents can be searched). This information is therefore not maintained in a system of records with and retrievable by unique identifier. Therefore, registration information on members of the public is not subject to a System of Record Notice. The FAA does not share information with any external entities regarding the registration information they collect in this spreadsheet.

Audit log information collected by the FAA to monitor and enforce access to the excel spreadsheet is used only as specified by the FAA's system of records notice, DOT/ALL 13, *Internet/Intranet Activity and Access Records*. The information collected in these audit logs only includes information on FAA employees, and not members of the public. In addition to other disclosures generally permitted under 5 U.S.C. §552a(b) of the Privacy Act, all or a portion of the records or information contained in this 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 approved investigations of improper access or usage of DOT computer systems;
- To an actual or potential party or his or her authorized representative for the purpose of negation or discussion of such matters as settlement of the case or matter, or informal discovery proceedings;
- To contractors, grantees, experts, consultants, detailees, and other non-DOT employees performing or working on a contract, service, grant cooperative agreement, or other assignment from the Federal government, when necessary to accomplish an agency function related to this system of records; and
- To other government agencies where required by law.

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

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).

Individuals registering for FAA Cyber Rodeo events manually input their own PII. This PII is therefore relied upon to be accurate. Users who need to update their data must email the system owner who will manually update the excel spreadsheet. The excel spreadsheet is downloaded daily from vFairs. Users can deactivate their account by emailing vFairs at tech@vfairs.com.

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 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).

vFairs implements administrative, technical, and physical measures to protect against loss, unauthorized access, or disclosure. The principle of least privilege is used to grant access to FAA federal employees and contractors who require access to the registration Excel spreadsheet. FAA's M365 SharePoint is also protected and requires employees and contractors have appropriate access credentials, such as a Personal Identity Verification (PIV) card.

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.

The FAA's AIS Security Governance Division is responsible for the administration of

FAA Order 1370.121B, *FAA Information Security and Privacy Program & Policy*. FAA Order 1370.121A defines the various privacy requirements of the *Privacy Act of 1974*, as amended (the Privacy Act), the *E-Government Act of 2002* (Public Law 107-347), the *Federal Information Security Management Act (FISMA)*, DOT privacy regulations, OMB mandates, and other applicable DOT and FAA information technology management policies and procedures. In addition to these, other policies and procedures will be consistently applied, especially as they relate to the access, protection, retention, and destruction of PII. Federal and contract employees are given clear guidance on their duties, as they relate to collecting, using, processing, and security privacy data. Guidance is provided in the form of mandatory annual security and privacy awareness training. In addition, staff are required to acknowledge understanding of the FAA Privacy Rule of Behavior (ROB) and agree to them before being granted access to FAA information systems. The DOT and FAA Privacy Offices will conduct periodic privacy compliance reviews of vFairs relative to the requirements of OMB Circular A-130, *Managing Information as a Strategic Resource*.

Responsible Official

Veronica Bunn
System Owner
Aviation Ecosystem Stakeholder Engagement Office
Office of the Chief Information Security Officer

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer