



U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration (FAA) Human Resource Management (AHR) FAA-Federal Human Resources Navigator (FAA-FHR)

Responsible Official

Jennifer Luttjohann
9-ACE-FAA-BENE@faa.gov
1-855-322-2363

Reviewing Official

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





Executive Summary

The Federal Aviation Administration's (FAA) Office of Human Resource Management (AHR), Benefits Operations Center (BOC) uses the Federal Human Resources Navigator (FAA FHR) to support the administration of FAA employee benefits and retirement programs. FAA FHR is authorized under Public Law 93-366, 5 United States Code (U.S.C.) 8350, and FAA Order 1100.1C and provides estimating tools for military and civilian retirement account deposits, as well as retirements and death benefits.

The FAA is publishing this Privacy Impact Assessment (PIA) for FAA FHR in accordance with Section 208 of the [E-Government Act of 2002](#) because the system processes personally identifiable information (PII) from members of the public, such as beneficiaries (spouses and children) of FAA employees.

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;*
- *Accountability for privacy issues;*

¹Office 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).



- *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

In the past, the FAA had multiple business processes that required the completion of various forms for FAA employee benefits and retirement programs. Pursuant to 5 U.S.C. § 8350 Retirement counseling, and [FAA Order 1100.1C](#) - *FAA Organization – Policies and Standards Document Information*, the FAA Office of Human Resource Management (AHR), Benefits Operations Center (BOC) implemented FAA FHR to automate complicated calculations and to help the BOC provide accurate retirement calculations, deposit calculations, and death benefits to FAA employees.

BOC specialists use the Retirement/Separation component of FAA FHR, which allows them to respond to requests for various retirement computations, and to make applications for Military Service Deposits, Civilian Deposit/Redeposits, and Death Benefits. Additionally, FAA employees have limited personal access to FAA FHR to input additional data, such as Thrift Savings Plan (TSP) information, and Social Security earnings for themselves and/or their spouse.

When a new FAA employee is on-boarded, their new employee information is transferred to the system via an electronic data exchange with the Department of Transportation CASTLE Interface Repository (CASTLE-IR) connection. This includes their name, date of birth (DOB), Social Security Number (SSN), Service Computation Date (SCD), and salary. This information is then updated each pay period to reflect any service or salary changes. This allows BOC employees to locate employees in the system and work with their records to provide the following retirement benefit services/documents, which are handled according to the National Archives and Record Administration (NARA) General Retention Schedules (GRS):

Request for Retirement Estimates:

The BOC staff may calculate a FAA employee's (requestor) retirement estimate upon the employee's request. The request submission is assigned as a case within the My Information Technology Service Management (MyITSM), which is an application that provides automated workflow management to track, manage, and administer BOC services. Should the request require generation of an annuity estimate, the BOC specialist opens the



requestor's record in FAA FHR and compares the service history data to the request as well as the requestor's electronic Official Personnel Folder (eOPF). This connection provides data from the Federal Personnel and Payroll System (FPPS) to FAA FHR. Next, the BOC specialist utilizes the information provided by the employee on the FAA 2730-1 Form to select the type of retirement scenario and options requested and runs the retirement annuity estimate by manually populating the data elements from the form into FAA FHR. Once the Benefits Operations Center Case Management Module (BOC CMM) calculations are completed, the system generates the estimate, and the BOC specialist sends it to the requestor via encrypted email in Portable Document Format (PDF) or by fax or mail. A copy of the generated estimate is maintained within FAA FHR.

Death Benefits for Members of the Public who are FAA Employee's Spouses and/or Beneficiaries:

The beneficiary of a deceased employee may make an Application for Death Benefits to the BOC. In most instances, the BOC Specialist will call the beneficiary and assist with completion of a Standard Form (SF) 3104. Beneficiary information, such as name, DOB, and address is input into the electronic forms creator² in FAA FHR. After obtaining the necessary information from the beneficiary, the BOC Specialist finalizes the form and mails it to them for signature. The beneficiary then reviews the form, adds any missing information manually, and attaches any required documentation (i.e., death certificate) along with their wet signature, and mails the package back to the BOC. A digital copy is maintained in the FAA's MyITSM system for one year. The BOC then forwards the completed, hardcopy package to the Department of Interior (DOI) via the FedEx.

Civilian or Military Deposit Estimate

The BOC staff may calculate a FAA employee's (requestor) military or civilian deposit estimate upon the employee's request. The request submission is assigned as a case within MyITSM, which provides automated workflow management to track, manage, and administer BOC services. The BOC specialist opens the requestor's record in FAA FHR and compares the service history data to that found in the requestor's electronic Official Personnel Folder (eOPF). The BOC specialist updates service history data in FAA FHR, calculates the military or civilian deposit in FAA FHR, and creates Standard Form SF – 2803 Application to Make Deposit or Redeposit or SF-3108 Application to Make Service Credit Payment (Federal Employees Retirement System). The BOC specialist then emails the form along with the calculation and instructions on how to pay the deposit to the employee via encrypted email in PDF, fax, or mail. A digital copy is maintained in the FAA's MyITSM system for one year.

² There are 16 OPM or FAA approved forms used to provide various retirement/benefits services.



Employee Benefits Center (EBC)

FAA employees also use their personal access to FAA-FHR to create customizable retirement scenarios at their convenience using this information, such as, with the new EBC module. EBC allows active, current FAA employees to create financial planning scenarios combining Federal retirement, private savings, and their spouse's retirement information into one source to produce a complete retirement picture and understand the likelihood of meeting their retirement income goals. The FAA employee logs into FAA FHR using their PIV or username/password, then enters their PII (e.g., SSN and DOB), and/or their spouse's PII (e.g., DOB and SSN), and is then able to use the module to run financial planning scenarios. The scenarios are saved in the system, the same as when the FAA FHR program creates estimates on behalf of employees using the existing Retirement/Separation module.

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) v3³, 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 Organizations⁴.

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.

FAA FHR is a privacy-sensitive system because it maintains, collects, uses, disseminates, and retains PII from FAA employees and their beneficiaries (such as spouses and children) who are members of the public to process retirement and benefits forms. The PII is collected directly from the FAA employee via forms, which are ultimately used in other AHR systems and the employee's eOPF. The FAA provides a Privacy Act Statement (PAS) on both the

³ <http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf>

⁴ http://csrc.nist.gov/publications/drafts/800-53-Appendix-J/IPDraft_800-53-privacy-appendix-J.pdf



forms and in the FAA FHR system to individuals from whom the program collects PII. The PAS describes the purpose and details the authority under which the PII is collected and informs individuals that the services they request may not be able to be provided if they do not provide the requested information.

The FAA/DOT limits the scope of PII collected in FAA FHR to support the purpose listed in the Department's Published System of Records Notice (SORN) [OPM/GOVT-1, *General Personnel Records*, 71 FR 35342 \(June 19, 2006\)](#). The FAA protects records subject to the Privacy Act in accordance with the SORN OPM/GOVT 1, which covers personnel records, including records related to federal benefits. This SORN covers current and former federal employees and their beneficiaries, who are members of the public, and covers maintaining the basic factual data about a person's Federal employment while in the service and after his or her separation.

[SORN DOT/ALL 13, *Internet/Intranet Activity and Access Records*, 67 FR 30757 \(May 7, 2002\)](#) covers login credentials, audit trails, and security monitoring for FAA employees and contractors who are part of the Navigator program and/or manage the system.

The publication of this PIA demonstrates DOT's commitment to providing appropriate transparency into the FAA-FHR system.

Individual Participation and Redress

DOT should provide 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 be provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

Data maintained in FAA FHR is primarily collected directly from the employee or from the Department or FAA systems authorized for this purpose. This is done through the FAA FHR and DOT's CASTLE-IR data exchange, which includes information such as salary history, employment service history, employee name, facility address, SSN, and DOB. The data in CASTLE-IR is initially obtained directly from the employee when they are hired and is updated as needed throughout the employee's career as their salary, position, and employment information at the FAA change. This data is available to employees via any SF-50 Notification of Personnel Action that they receive in their eOPF.

Some death beneficiary information is maintained in FAA FHR. As discussed above, when an employee dies, in most cases, the BOC calls beneficiaries to assist them with completing death benefits applications. Their information is input into the FHR electronic forms creator



and then the forms are sent to the beneficiaries for completion. If there are errors on the form(s), beneficiaries may contact the BOC, and information will be updated.

FAA employees and their beneficiaries may request their benefits or retirement information be updated, amended, or changed by contacting a BOC specialist by phone (1-855-322-2363), email (9-ace-FAA-bene@faa.gov), fax (816-329-2418 or 816-329-2476), or postal mail (BOC, 901 Locust Street, Kansas City, Missouri 64106). If updates to information maintained in CASTLE-IR are necessary, the employee should contact their local HR office.

Under the provisions of the Privacy Act, individuals may request searches of agency records to determine if any added records pertain to them. Individuals wishing to know if their records appear in this system may inquire in person or in writing to:

Federal Aviation Administration
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

Individuals seeking to contest information about them that is contained in FAA FHR should make their request in writing, detailing the reasons their records must be corrected and addressing their letter to the following address:

Federal Aviation Administration
Privacy Office
800 Independence Avenue, SW
Washington, DC 20591

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 authorized the FAA Administrator to develop systems and/or tools to provide benefits and retirement services. FAA FHR addresses the unique demands of the FAA's workforce and operates under the following authorities:

- *Retirement Counseling*, 5 U.S.C. § 8350 empowers a federal agency, including the FAA, to appoint a "retirement counselor to furnish information on benefits and counseling services relating to such benefits to other employees of the agency." The retirement counselor is any employee of the agency designated by the head of the agency to furnish information on employee benefits, such as retirement and insurance benefits.
- FAA Order 1100.1C⁵ authorizes AHR to appoint, develop, and sustain employees through human resources programs including...compensation and benefits, and ... to develop and manage total rewards programs to recruit, retain, and engage employees including benefits. The information collected on the OPM forms maintained in the BOC CMM, is authorized by 5 U.S.C, Sections 1302, 2951, 3301, 3372, 4118, Chapters 83 and 84.

FAA FHR collects PII for the following purposes:

- For FAA FHR access and program management from FAA employees and contractors: Name, business email, username, and password.
- For benefits and retirement counseling from members of the public (FAA employee's spouses and beneficiaries): full name, DOB, SSN, position history, address, and job title.

FAA-FHR uses this information in accordance with the purposes for which it is collected under SORNs:

- [OPM/GOVT-1, *General Personnel Records*, 71 FR 35342 \(June 19, 2006\)](#) for benefits and retirement counseling and processing retirement, death in service, and civilian/military deposit actions.
- [DOT/ALL 13, *Internet/Intranet Activity and Access Records*, 67 FR 30757 \(May 7, 2002\)](#) for login credentials, audit trails, and security monitoring for

⁵ FAA Order 1100.1C -

https://www.faa.gov/regulations_policies/orders_notices/index.cfm/go/document.information/documentID/1040403.



FAA employees and contractors who are part of the FAA FHR program and/or manage the system.

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 manages risk by limiting the amount of PII collected by FAA FHR to the information relevant and necessary to assist the BOC in processing retirements, retirement estimates, civilian/military deposits, and death in service actions.

Prior to working with FAA employees, BOC staff use the full name, DOB, and last four digits of the SSN to validate the employee's identity. Each FAA FHR user must annually sign the FAA FHR Rules of Behavior, which states that they "acknowledge that the Privacy Act of 1974, as amended, applies to all protected information contained in FAA FHR and that they will comply with numerous privacy and security requirements. If a FAA FHR user does not agree to the FAA FHR Rules of Behavior, a FAA FHR Administrator will revoke that user's access.

Records in the system are maintained in accordance with following National Archives and Record Administration (NARA) approved General Retention Schedules (GRS):

- [NARA GRS 2.5, Approved January 2017, Employee Separation Records](#), Item 020 *Individual Employee Separation Case Files*. These records are temporary and should be destroyed 1 year after date of separation or transfer, but longer retention is authorized if required for business use.
- [NARA GRS 3.2, Approved September 2014, Information Systems Security Records](#), Item 030, *System Access Records*, which covers login credentials, audit trails, and security monitoring. 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.

FAA FHR is used to calculate civilian/military service deposits, process deposit, retirement, and death in service forms, and calculate retirement benefits estimates for FAA employees and members of the public (FAA employees' spouses or beneficiaries). PII collected by FAA FHR is used only for the purposes of completing these forms and calculating these benefits.



FAA FHR administrators and senior staff provide user guides, as well as train staff on the use of FAA FHR data and other PII. Employees agree, in accordance with the annual FAA FHR Rules of Behavior that they are required to sign, to stay current on information technology (IT) security and privacy awareness training, to protect their Personal Identity Verification (PIV) card and not leave them unattended, to protect PII from disclosure to unauthorized persons or groups, and to lock their computers whenever they step away from them.

The FAA/DOT limits the scope of PII collected in FAA FHR to support the purpose specified in SORN [OPM/GOVT-1, *General Personnel Records*, 71 FR 35342 \(June 19, 2006\)](#).

Access and authentication records within FAA FHR are handled in accordance with SORN [DOT/ALL 13, *Internet/Intranet Activity and Access Records*, 67 FR 30757 \(May 7, 2002\)](#)

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).

Employees are responsible for ensuring the accuracy of the information that the employee provides on their SF 50, "Notification of Personnel Actions" from their eOPF. Employees provide information such as name, date of birth, and SSN when they are initially hired. This data, along with other personnel data (salary, pay plan, series, grade, etc.) is obtained via the FAA FHR CASTLE-IR data exchange, and is used to automatically populate FAA FHR. The data is updated biweekly, ensuring that the most up-to-date information is provided in FAA FHR.

The BOC specialist validates all employees' information prior to working on their benefits actions in FAA FHR. They must input the employee's name or SSN to locate them in the system, and this information must be input correctly to locate their information.

BOC Administrators enforce rigorous access controls. Only trained BOC staff who have agreed to the Rules of Behavior are given access to FAA FHR. Once BOC employees separate, their access to the system is immediately revoked. When an employee or contractor leaves the FAA, an administrator removes their system access. Administrators also review the audit logs monthly to ensure there are no unauthorized logins.

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 the National Institute of Standards and Technology Special Publication (NIST) 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, dated September 2020.

These safeguards include an annual independent risk assessment of the FAA FHR system to test security processes, procedures, and practices. The system operates on security guidelines and standards established by the National Institute of Standards and Technology (NIST), and the FAA FHR system owner restricts access to the records in FAA FHR to only FAA personnel with a need to know authorized to access. 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 processes, procedures, and posture of the system. System audit logs are reviewed monthly to monitor for unauthorized use.

BOC Specialists access FAA FHR via their PIV card. They are required to complete annual security and privacy awareness training and role-based training. The training teaches individuals to understand how privacy influences their roles and to perform their duties properly and securely in situations involving the use of PII. Necessary clearances and completion of required security and privacy training allows for access to FAA FHR for BOC users.

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 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.



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.

In addition to these practices, the FAA will implement additional policies and procedures as needed as they relate to the access, protection, retention, and destruction of PII. Federal employees and contractors who work with FAA FHR 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, as well as FAA Order 1370.121B. The FAA conducts periodic privacy compliance reviews of FAA FHR consistent with the requirements of OMB Circular A-130, *Managing Information as a Strategic Resource*.

Responsible Official

Jennifer Luttjohann
System Owner
Director, Benefits Operations and Planning

Prepared by: Barbara Stance, FAA Chief Privacy Officer

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer