U.S. Department of Transportation

Privacy Impact Assessment

Human Resources Management (AHR)

Office of Workers Compensation Program Tracking System (OWCP)

Responsible Official

Aaron Anthony
Email: Aaron.Anthony@faa.gov
Phone Number: 703-230-7664 ext. 3252

Reviewing Official

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

Executive Summary

The Office of Workers Compensation Program Tracking System (OWCP) serves as a consolidated database that maintains information used by the Federal Aviation Administration (FAA) to track and manage all DOT workers' compensation claims, including medical claim history and treatment. The OWCP administers four major disability compensation programs: the Federal Employees' Compensation Program (FECA), the Longshore and Harbor Workers' Compensation Program, the Energy Employees Occupational Illness Compensation Program (DEEOIC), and the Black Lung Benefits Program. These compensation programs provide wage replacement benefits, medical treatment, vocational rehabilitation, and other benefits to certain workers or their dependents who experience work-related injury or occupational disease.

The Office of Workers' Compensation Programs seeks to protect the interests of workers who are injured or become ill on the job, their families and their employers by making timely, appropriate, and accurate decisions on claims, providing prompt payment of benefits, and helping injured workers return to gainful work as early as is feasible.

The FAA is updating and publishing this Privacy Impact Assessment (PIA) for the OWCP in accordance with Section 208 of the E-Government Act of 2002 because the OWCP processes Personally Identifiable Information (PII) from members of the public, including citizens or Legal Permanent Residents (LPR).

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.*
- *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 Human Resources Management Information Technology Applications (AHR-IT) developed OWCP to address the unique demands of the DOT's workforce and operates under the authority of the Federal Employee's Compensation Act (FECA) as amended 5 U.S.C. chapter §8101 et seq, Title 20 Code of Federal Regulation (CFR), Chapter 1. FECA establishes the system for processing and adjudicating claims that Federal employees and other covered individuals file with the Department's OWCP. The FAA's Human Resource Management uses OWCP to manage and track DOT employees' workers' compensation claims. In cases involving disability or disputed claims, the FAA uses OWCP to monitor case status and facilitate the employee's return to work. Supervisory Human Resource Specialists in the AHB-300, Worker's Compensation division of the Office of Human Resources (AHR), hereafter referred to as AHB-300, maintain a caseload of claims, oversee active cases, and work cases to resolution.

The system contains PII including names, addresses, email addresses, and phone numbers of DOT employees and members of the public, who are third parties including caregivers,

[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).

spouses, attorneys, witnesses to an event, or other individuals who may be associated with the DOT employee filing a claim.

Only FAA employees and contractors of AHB-300, specifically analysts in the office of human resources, have access to the system. When new FAA AHB-300 employees in the office of Human Resources are on boarding, they must contact the system owner to request access to the OWCP system. The system owner reviews the request and grants access through the following uniform resource locator (URL): https://ahrweb.faa.gov/owcp/. Users must authenticate using their Personal Identity Verification (PIV) card through MyAccess. The OWCP receives the username and FAA email address from MyAccess for access and authentication.

Typical Transaction:
The typical transaction begins when AHB-300 receives an email containing an employee's name, Employee's Compensation Operations and Management Portal (ECOMP) Control Number (ECN #), and type of form filed (CA-1 Notice of Traumatic Injury and Claim for Continuation of Pay/Compensation or CA-2 Notice of Occupational Disease and Claim for Compensation), from the Department of Labor's (DOL) OWCP (ECOMP) alerting the FAA AHB-300 that a DOT employee, referred to as a "claimant," filed a claim. The email goes to all staff (approximately 15) in AHB-300 who process claims.

AHB-300 receives a second email once the employee's manager completes their portion of the claim form, as required. After the initial notification, but particularly after the manager's completion notification, AHB-300 staff members assigned to the case may access the claim record in ECOMP to review the claim to ensure accuracy before AHB-300 certifies it and transmits it to DOL for action. DOL does not act on a claim until the FAA finalizes its review and submits it. Once the claim is accurate, AHB-300 transmits the claim via ECOMP to DOL, then adds the claim into OWCP by accessing the claim in ECOMP and manually enters information about the claimant from the ECOMP record into OWCP Tracking System, including the DOT employee name, date of injury, region or DOT operating administration, Line of Business (LOB), ECOMP Control Number, and DOL Claim Number. The FAA has established appropriate data-sharing agreements.

The "Notes" section may include the claimant's medical status, updates on the case, summaries of conversations, and any correspondence, including emails or discussions. It may also include the PII of third parties such as caregivers, spouses, attorneys, witnesses to an event, or other individuals who may be associated with the DOT employee filing a claim. Throughout the workers' compensation claims process, FAA employees from AHB-300

may access the DOL's ECOMP system at various stages to find new information that can be added to the claimant's record in the OWCP Tracking System.

Reports:

The OWCP generates reports based on various criteria. These reports may include aggregated data, including information on claims filed, resolved claims, case management actions taken on claims, and cost avoidance. Depending on the specific criteria of each report, the PII of both DOT/FAA employees (claimants) and OWCP staff may be included. PII elements can consist of name, regions, LOB/SO, hourly pay rate, date of injury, dates related to case management actions taken by DOL and/or DOT, and DOL Claim Number.

Audit Logs:

OWCP produces four audit reports, which may contain the following PII and other data:

- Login Report: username, login ID, user role (ex. admin), login date and time, logout date and time, modified date/time, and modified by (username)
- Error Report: username, user's role, error description, time of error, and page/screen (URL of page with error)
- Database Report: Username, user role, history ID, table name, modified date and time, action, and view
- Users Report: username, user ID, active flag

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

[2] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf
[3] https://csrc.nist.gov/publications/detail/sp/800-53a/rev-5/final

impact of government programs and activities. Accordingly, DOT is open and transparent about policies, procedures, and technologies at 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 uses several methods to inform individuals about its information collection and usage practices. The DOT and FAA System of Record Notices (SORNs) provide transparency about privacy practices regarding the collection, use, sharing, safeguarding, maintenance, and disposal of information about individuals covered under the Privacy Act of 1974 as amended. The Department provides public notice of information collected in OWCP through the following Privacy Act System of Records Notices (SORNs):

- **DOL/GOVT-1, Office of Workers' Compensation Programs, Federal Employees' Compensation Act File (81 FR 25776, April 29, 2016):** This SORN includes injury reports from employees or their agencies and claim forms for FECA benefits. It covers forms for medical care, other medical records and reports, payment records, and compensation payment records. It also includes benefit payment decisions, hearing transcript**s,** and any information related to the claim, like medical, employment, or personal details. This SORN applies to the PII above for both the public and DOT employees in OWCP
- **DOT/ALL 13, Internet/Intranet Activity and Access Records (67 FR 30757, May 7, 2002):** Covers FAA access information records used for creating and validating login credentials, audit trails, and security monitoring for the OWCP program participants.

No Privacy Act Statement (PAS) is included because the DOT employee files the complaint through DOL. The publication of this PIA demonstrates DOT's commitment to provide appropriate transparency into the OWCP process to protect the interests of workers who are injured or become ill on the job, their families and their employers by making timely, appropriate, and accurate decisions on claims, providing prompt payment of benefits, and helping injured workers return to work as early as is feasible.

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.

OWCP maintains records obtained from members of the public, and the DOT Federal workforce. Individuals have the right to access, correct, or amend their information protected under the Privacy Act. DOL/GOVT-1, Office of Workers' Compensation Programs, Federal Employees' Compensation Act File, 81 FR 25776 (April 29, 2016) covers records retrieved using DOT employee/claimant name or DOL Claim number. Additionally, records created for the purposes of account creation, logging, auditing, etc. are covered by DOT/ALL-13. Individuals can request searches under the Privacy Act to see if any records pertaining to them have been included.

For all inquiries related to the information contained in the Office of Workers Compensation Program Tracking System the individual may appear in person, send a request via email (privacy@faa.gov) or in writing to:

AHB-300 OWCP Program Manager
Orville Wright Bldg. (FOB10A)
FAA National Headquarters
800 Independence Ave, 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 wanting to contest information about themselves that is contained in OWCP should make their requests in writing, detailing the reasons why the records should be corrected to the following address:

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

If you have comments, concerns, or need more information on FAA privacy practices, please contact the Privacy Division at privacy@faa.gov or 1 (888) PRI-VAC1.

Purpose Specification

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

The AHR-IT developed OWCP to address the unique demands of the DOT's workforce and operates under the authority of the FECA as amended 5 U.S.C. chapter §8101 et seq, 20 CFR Code of Federal Regulations. FECA establishes the system for processing and adjudicating claims that Federal employees and other covered individuals file with the Department's OWCP. The FAA's Human Resource Management uses OWCP to manage and track DOT employees' workers' compensation claims. In instances of disability or disputed claims, the FAA uses OWCP to monitor the case status and facilitate a return to work for the employee.

The OWCP sends or receives the following information to or from other FAA systems:

- The DOL ECOMP Portal sends the DOT employee name, date of injury, region or DOT operating administration, ECOMP Control Number, and DOL claim number from DOL ECOMP by email. FAA AHB-300 employees' access ECOMP and manually enter data from a claimant's record in ECOMP into OWCP. This process ensures the accuracy of the claim before AHB-300 certifies and transmits the claim to DOL for further action OWCP.
- MyAccess receives the FAA employee and contractor username and FAA email address to OWCP using HTTPS for authentication and providing access to the portal.

The FAA has established appropriate data-sharing instruments.

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 minimizes its maintenance, use, and retention within the OWCP to only what is relevant and necessary for its authorized business purpose. Records are maintained in accordance with the National Archive and Records Administration (NARA) General Records Schedule (GRS):

- **Workers' Compensation (personnel injury compensation) (GRS 2.4, Item 100, approved May 2024):** Temporary records forwarded to DOL for inclusion in DOL's master OWCP files. These are Federal Employees' Compensation Act case files on injuries federal employees sustain while performing their duties that result in lost time or death, regardless of whether the employee files a workers' compensation

claim. Destroy three years after compensation ceases or when the deadline for filing a claim has passed. Disposition Authority: DAA-GRS-2016-0015-0012.

- **Workers' Compensation (personnel injury compensation) (GRS 2.4, Item 101, approved May 2024):** These records are from agencies that do not forward case file material to DOL for inclusion in DOL's master OWCP records. They cover federal employees injured while at work who suffer lost time or death, regardless of whether a workers' compensation claim was filed. Content includes forms, reports, correspondence, claims, medical and investigatory records, administrative determinations or court rulings, and payment records. Temporary records must be destroyed 15 years after compensation ceases or when the deadline for filing a claim has passed. Disposition authority: DAA-GRS-2016-0015-0013.

All other records maintained in OWCP, which are record copies from other FAA systems (not case files), are maintained in accordance with the National Archive and Records Administration (NARA) General Records Schedule (GRS):

- **Information Systems Security Records (GRS 3.2 Item 30, approved January 2023)** These are created during user identification and authorization process for system access. Records are destroyed when business use ceases. Disposition authority: DAA -GRS-2013-0006-0003.
- **Information System Security Records (GRS 3.1, Item 20 approved November 2019)**These are technology and maintenance records. Destroy three years after the agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated or superseded. Retain longer if needed for business. DAA-GRS 2013-0005-0004.

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 PII in Office Worker's Compensation Program system is used to be able to track compensation cases and used for only that purpose. The system creates or makes previously unavailable information available about an individual in the medical report information from members of the Public, and the DOT Federal workforce. The FAA does not use the PII for any other purpose.

The FAA limits the scope of PII collected in Office Worker's Compensation Program system covered under SORNs: DOL/GOVT-1, Office of Workers' Compensation Programs, Federal Employees' Compensation Act File, 81 FR 25776 (April 29, 2016),

GOVT-1 Routine Uses are as follows:

To Federal agencies that employed the claimant at the time of the occurrence or recurrence of the injury or occupational illness in order to verify billing, to assist in administering FECA, to answer questions about the status of the claim, to consider rehire, retention or other actions the agency may be required to take with regard to the claim or to permit the agency to evaluate its safety and health program. Disclosure to Federal agencies, including the Department of Justice, may be made where OWCP determines that such disclosure is relevant and necessary for the purpose of assisting in asserting a defense based upon FECA's exclusive remedy provision to an administrative claim or to litigation filed under the Federal Tort Claims Act.

- To other Federal agencies, other Government or private entities and to private-sector employers as part of rehabilitation and other return-to-work programs and services available through OWCP, where the entity is considering hiring the claimant or where otherwise necessary as part of that return-to-work effort.
- To a Federal, State or local agency for the purpose of obtaining information relevant to a determination concerning initial or continuing eligibility for FECA benefits, and for a determination concerning whether benefits have been or are being properly paid, including whether dual benefits that are prohibited under any applicable Federal or State statute are being paid; and for the purpose of utilizing salary offset and debt collection procedures, including those actions required by the Debt Collection Act of 1982, to collect debts arising as a result of overpayments of FECA compensation and debts otherwise related to the payment of FECA benefits.
- To a Federal, State or local agency charged with the responsibility for investigating compliance with laws relating to health and safety, for the purpose of assisting such agency in fulfilling its statutory or regulatory responsibilities.

The sharing of user account information within the OWCP system are handled in accordance with SORN DOT/ALL 13- Internet/Intranet Activity and Access Records, 67 FR 30757 (May 7, 2002).

DOT/All 13 Routine Uses are as follows:

- To provide information to any person authorized to assist in an approved investigation 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 negotiation or discussion of such matters as settlement of the case or matter, or informal discovery proceedings.

- To contractors, grantees, experts, consultants, detailers, 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.
- To other government agencies where required by law.
- See Prefatory Statement of General Routine Uses.

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).

The FAA collects, uses, and retains relevant data as necessary for its intended purposes. The FAA relies on the information's accuracy, as AHB-300 employees manually enter the PII from a claimant's record in ECOMP into the OWCP system. This process ensures the claim's accuracy before the AHB-300 employee certifies it and transmits it to DOL for action.

The AHB-300 employees exclusively use the data entered in this system to track compensation cases. The application software includes validation checks that prompt users to correct incorrect entries and confirm successful data input.

The OWCP implements appropriate security measures to protect sensitive information. These measures include intranet access only and limited system access to 15 authorized employees of AHB-300. The OWCP system is in a controlled computer center within a secure facility. Physical access to the OWCP system is limited to authorized personnel who use photo badges, building key cards, and room-access keypads. The OWCP applies DOT security standards, which consist of routine scans and monitoring, backup activities, and background security checks for technical employees and contractors.

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 (includes updates as of Dec. 10, 2020).

These safeguards include an annual independent risk assessment of the OWCP system to test security processes, procedures, and practices. The system operates on security guidelines and standards established by NIST; only FAA personnel needing to know are authorized to access the records in the OWCP system. All data in transit is encrypted, and access to electronic records is controlled by PIV, Personal Identification Number (PIN), and limited according to job function. Additionally, the FAA conducts an annual cybersecurity assessment to test and validate the system's security process, procedures, and posture. Based on security testing and evaluation in accordance with FISMA, the FAA issues the OWCP system authorization to operate.

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 Office of the Chief Information Officer, Office of Information System Security Privacy Division is responsible for governance and administration of FAA Order 1370.121B, FAA Information Security and Privacy Program and Policy," FAA Order 1370-121B 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.

DOT 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.

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 Office Worker's Compensation Program

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 Office Worker's Compensation Program as related to the requirements of OMB Circular A-130, "Managing Information as a Strategic Resource."

Responsible Official

Aaron Anthony
System Owner, Federal Aviation Administration (FAA)

Approval and Signature

Karyn Gorman
Chief Privacy Officer KARYN MARIE GORMAN Digitally signed by KARYN MARIE GORMAN Date: 2026.05.29 13:26:22 -04'00'
Office of the Chief Digital & Information Officer