U.S. Department of Transportation

Privacy Impact Assessment

Office of the Secretary (OST)

Office of Human Resource Management (M-10)

Worker's Compensation Information System (WCIS)

Responsible Official

Stacy McDaniel
stacy.mcdaniel@dot.gov
Phone Number: 202-366-3144

Reviewing Official

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

Executive Summary

The Department of Transportation (DOT) uses the Workers' Compensation Information System (WCIS) to manage the Department's workers' compensation program. It allows authorized personnel to manage and monitor workers' compensation claims data cases. Data in the WCIS is provided by the United States Department of Labor (DOL) under the Federal Employee Compensation Act (FECA). The DOT Office of Human Resource Management manages WCIS.

This Privacy Impact Assessment (PIA) is being updated in accordance with the E-Government Act of 2002 to address potential privacy risks regarding the Personally Identifiable Information (PII) of federal employees and members of the public who receive benefits from WCIS.

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;*

[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).

- *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

WCIS allows case workers and managers to monitor the status of worker's compensation cases established with the United States Department of Labor (DOL) under the Federal Employee Compensation Act (FECA). The information received in WCIS from the DOL contains PII from the following forms: CA-1: Federal Employee's Notice of Traumatic Injury and Claim for Continuation of Pay/Compensation, CA-2: Notice of Occupational Disease and Claim for Compensation, and CA-6: Official Superior's Report of Employee's Death. These forms include information on members of the public and members of the DOT federal workforce. The DOL assigns each case a claimant case number in its Employees' Compensation Operations & Management Portal (eCOMP) system. The Social Security Number (SSN) is used to identify the compensation claims between the two systems. The authority to collect is governed by 5 U.S.C. 7901, Health Service Programs; 21 U.S.C. 1101, Food and Drugs, Congressional findings; 42 U.S.C. 4541, Public and Welfare, Congressional findings and declaration of purpose; 5 U.S.C. 8101 et seq., Government Organization and Employees: Definitions; 5 U.S.C. Chapter 81, Compensation for Work Injuries; 20 CFR 1.1 et seq. The Office of Workers' Compensation Programs operate under the authority of E.O. 9397 (SSN), as amended. Claims payment information is updated using sensitive personally identifiable information that includes (SPII) the SSN and is required to file a claim as stated in the DOL/GOVT-1, Office of Workers' Compensation Programs, Federal Employee Compensation File, 81 FR 25776, April 29, 2016.

Department of Labor Forms CA-1, CA-2, and CA-6 contain the following PII:

- Employee name
- Email address
- Social Security Number
- Date of Birth
- Sex
- Home Telephone
- Mailing Address
- Dependents
- Spouse/next of kin name and address
- Physician's Name

- Physician's Address
- Supervisor Name
- Supervisor's Title

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 information practices within an organization 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.

Records in the system are retrieved by personal identifier are subject to the provisions of the Privacy Act of 1974. Records are maintained in accordance with the Departments published System of Records Notice (SORN), DOT/ALL 6, Workers Compensation Information System, 65 FR 19480, April 11, 2000. There are no exemptions claimed for the system. PII shared with the Department of Labor are covered in a routine use under DOT/ALL 6, Workers Compensation Information System, system of records notice.

Records in this system are also covered by DOL/GOVT-1, Office of Workers Compensation Programs, Federal Employees Compensation Act File, 81 FR 25776, April 29, 2016. There is an exemption claimed in DOL/GOVT-1 in accordance with 5 U.S.C. 552a (k)(2), investigative material in this system of records compiled for law enforcement purposes (e)(1), (e)(4)(G), (H) and (I), and (f) of 5 U.S.C. 552a, provided, however, that if any individual is denied any right, privilege, or benefit that he or she would otherwise be entitled to by Federal law, or for which he or she would otherwise be eligible, as a result of the

[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

maintenance of these records, such material shall be provided to the individual, except to the extent that the disclosure of the material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or prior to January 1, 1975, under an implied promise that the identity of the source would be held in confidence. Refer to DOT/ALL 6, Workers Compensation Information System, 65 FR 19480, April 11, 2000, for additional routine uses covered by this system.

The following PII elements are collected for this system:

- Employee name
- Email address
- Social Security Number
- Date of Birth
- Sex
- Home Telephone
- Mailing Address
- Dependents
- Spouse/next of kin name and address
- Physician's Name
- Physician's Address
- Supervisor Name
- Supervisor's Title

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.

Authorized users that have a need to know can access WCIS from their desktop computer and obtain immediate access to up-to-date, comprehensive information on all cases for which they have managerial responsibility. The SORNs that maintain these records are listed above in the Transparency section.

Under the provision of DOT Privacy Act/Freedom of Information Act (FOIA) procedures, individuals may request searches of WCIS to determine if any records may have been added or pertain to them. The FOIA is a federal law that gives you the right to access any DOT records unless DOT reasonably foresees that the release of the information to those records would harm an interest protected by one or more of the nine exemptions (such as classified

national security, business proprietary, personal privacy, investigative documents) or release is prohibited by law. DOT will review all Privacy Act Requests on an individual basis and may waive exemptions if the release of information to the individual would not cause harm to applicable exemptions such as law enforcement or national security.

Record Access and Notification procedures:

Requests should be submitted to the attention of the official responsible for the record at the address below:

Director
National Workers' Compensation Program (AHB-300)
U.S. Department of Transportation
Human Resource Management (AHR)
Federal Aviation Administration
800 Independence Ave, SW
Washington, DC 20591
Email: 9-AWA-AHR-OWCP-Claims@faa.gov
Fax: 202-267-6295

Individuals should include in their requests the following information:

- Name and title of the system of records from which you are requesting the search.
- Name of DOT component or office where you worked
- Name of individual
- Mailing address
- Phone number or email address; and
- Description of the records sought, and if possible, location of records.

Contesting record procedure: Individuals wanting to contest information about themselves contained in this system should make their requests in writing, detailing the reasons for and why the records should be corrected. Requests should be submitted to the attention of the OST Official responsible for the record at the address listed in the records access and notification section above.

Privacy Act request for records notices not published by the Department will be coordinated with the appropriate customer privacy official and acted upon accordingly.

Additional information about the Department's privacy program may be found at: https://www.transportation.gov/privacy-program/about-us. Individuals may also contact the DOT Chief Privacy Officer at: privacy@dot.gov. For questions relating to DOT's Privacy Program please go to http://www.dot.gov/privacy.

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 its collects, uses, maintains, or disseminates PII.

Federal Employee Compensation Act (FECA) establishes the requirements for WCIS to process and adjudicate claims that Federal employees and other covered individuals file with the DOL's Office of Workers' Compensation Programs (OWCP) seeking monetary, medical, and similar benefits for injuries or deaths sustained while in the performance of duty. WCIS establishes and maintains an automated data/information base that is used to improve claims management of the Federal Employees Compensation program within the Department; develop policy guidance; and promote training programs. The records provide information and verification about the individual's employment-related injury and the resulting disabilities and/or impairments, if any, on which decisions awarding or denying benefits provided under the FECA must be based.

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. DOT should retain PII for only if necessary to fulfill the specified purpose(s) and in accordance with a National Archives and Records Administration (NARA)-approved record disposition schedule.

Claims data, which is entered into the DOL eComp system and quarterly chargeback data is received from DOL on a biweekly and quarterly basis respectively. WCIS monitors the status of workers' compensation cases established with DOL under FECA. The claimant volunteers to share PII through e-COMP and ultimately to the WCIS for processing and monitoring with the goal of being compensated for their injury or illness.

DOT WCIS manages risk by providing only relevant and necessary PII to conduct, manage, and process requests for WCIS. WCIS shares SSNs and additional PII collected from eCOMP in listed in forms CA-1, Federal Employee Notice of Traumatic Injury and Claim for Continuation for Pay/Compensation, CA-2, Notice of Occupational Disease and Claim for Compensation, and CA-6, Official Superior Report of Employee's Death.

Records in WCIS are retained in accordance with National Archives and Records Administration (NARA) record schedules as follows:

- *GRS 2.4, Employee Compensation and Benefits Records:* Item 100, DAA-GRS-2016-0015-0012, Temporary. Destroy 3 years after compensation ceases or when deadline for filing a claim has passed. Item 101, DAA-GRS-2016-0015- 0013, Temporary. Destroy 15 years after compensation ceases or when deadline for filing a claim has passed.

- *GRS 4.2: Information Access and Protection Records:* Item 140: DAA-GRS2013-0007- 0013, Temporary. Destroy when business use ceases.

- *GRS 5.2, Transitory and Intermediary Records:* Item 010, DAA-GRS-2022-0009-Temporary. Destroy when no longer needed for business use, or according to an agency predetermined time period or business rule.

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.

Data collected is shared with the appropriate systems within DOT. Data encryption is applied to storage and transmittal. WCIS collects PII because it is required to link for verification, to maintain a historical records, and manage claim payments made to a claimant. Records in the system are covered under the following System of Record Notices:

- DOT/ALL 6 – Workers Compensation Information System – 65 FR 19480 – April 11, 2000
- DOL/GOVT-1 Office of Worker's Compensation Programs Federal Employees' Compensation Act File FR 25776, April 29, 2016

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).

PII collected directly from the individual and DOT records, align with the purpose of SORNs DOT/ALL 6 and OPM GOVT-1. Claimants are responsible for ensuring the accuracy quality of data provided for processing. Records in this system are used to process claims. WCIS employs the data accuracy checks in its database software to ensure data validity and accuracy. The system is reviewed to ensure, to the greatest extent possible, it is accurate, relevant, timely, and complete via security testing and evaluation. Only authorized individuals have access to WCIS. Access to data in the system is managed through user roles and limited to those that have a need to know.

Security

DOT shall implement administrative, technical, and physical measures 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.

In accordance with FECA, the PII collected within the data repository is stored via encrypted means and transmitted via secured transmission methodologies.

PII is protected by 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 System 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 NIST Special Publication (SP) 800-53 as revised, Recommended Security Controls for Federal Information Systems and Organizations, dated August 2009. The Department has a comprehensive information security program that contains management, operational, and technical safeguards that are appropriate for the protection of PII. These safeguards are designed to achieve the following objectives: Ensure the security, integrity, and confidentiality of PII:

- The WCIS system has an annual Continuous Monitoring Assessment (CMA) process that supports reaccreditation/reauthorization of the system. Each year's CMA addresses the OMB Circular A-130 requirement for annual testing.
- Encryption of PII which is stored and/or transmitted is compliant with FIPS 140-2 standards.
- WCIS personnel handling sensitive information are required to undergo appropriate background checks to assess their suitability to perform in public trust positions. Additionally, all staff undergoes initial security awareness training and annual refresher training, and the procedures for properly protecting the privacy of users' personal information are stressed in this training.

WCIS is designed to meet all current cyber security requirements for protecting privacy information while still allowing only authorized users the full transparency needed to complete the personnel security process for applicants, employees, and contractors. WCIS records are safeguarded in accordance with applicable rules and policies, including all applicable Department automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in WCIS is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances and permissions. WCIS is protected from unauthorized access through appropriate administrative, physical, and technical safeguards and all system access is logged and monitored.

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.

WCIS audit logs are periodically reviewed for any anomalies. The WCIS auditing system captures account maintenance and events. The Information System Owner (ISO), Information Systems Security Manager (ISSM) and/or DOT Security Operations Center (SOC) will determine the frequency and any changes which need to occur on the system due to the current threat environment. Only authorized system, database, and application administrators have rights sufficient to access audit logs based on their roles. The logged auditable events are adequate to support after-the-fact investigations.
WCIS Rules of Behavior documents are in place that outline specific guidelines for usage of WCIS. Users of the system acknowledge and understand their roles and responsibilities relative to access and usage of the data in the system. The DOT Order 1351.37 Departmental Cybersecurity Policy ensures that the WCIS ISO is responsible for ensuring information system security awareness training is provided to new employees automatically, and re-assigned annually, to employees and contractors with access to WCIS. Personnel who are assigned to a DOT project with access to DOT information or information systems complete annual security awareness training and that evidence of completion is obtained and provided to the appropriate Information System Security Officer (ISSO) or Information System Security Manager (ISSM).

Responsible Official

Stacy McDaniel
Information System Owner
Associate Director - HR Systems,
Department of Transportation

Approval and Signature

Karyn Gorman
DOT Chief Privacy Officer
Office of the Chief Information Officer

KARYN MARIE GORMAN
Digitally signed by KARYN MARIE GORMAN
Date: 2025.04.23 13:04:11 -04'00'