U.S. Department of Transportation

Privacy Impact Assessment

Office of the Secretary (OST)

Office of Human Resource Management (M-12)

Federal Personnel Payroll Systems (FPPS) Web Printing System (WPS)

Responsible Official

Stacy McDaniel
Associate Director, HR Systems, OST M-12
Email: Stacey.McDaniel@dot.gov
Phone Number: (202) 366-3314

Reviewing Official

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

Executive Summary

The Federal Personnel Payroll Systems (FPPS) Web Printing System (WPS) is a Department of Transportation (DOT) Office of the Secretary (OST) owned system that provides the ability to generate and print the notification of personnel action form SF-50 and request for personnel action form SF-52. WPS contains Personally Identifiable Information (PII) on current and former (including retirees) DOT employees that is shared from the FPPS which is owned by the Department of Interior (DOI). The authority to collect and share PII in WPS is covered under 31 U.S.C. 3512, Executive agency accounting and other financial management reports and plan; 5 U.S.C. 1302, Regulations; 5 U.S.C. 2951, Reports to the Office of Personnel Management; 5 U.S.C. 3301, Civil service; generally; 5 U.S.C. 3372, General provisions; 5 U.S.C. 4118, Government Organizations and Employees; U.S. C. 8506, Dissemination of information; 5 U.S.C. 8347, Administration; regulations; Executive Order (E.O.) 9397,(SSN), as amended.

This Privacy Impact Assessment (PIA) was developed pursuant to Section 208 of the E-Government Act of 2002 because the WPS uses and shares PII. This document serves as an update to the previous PIA to address the privacy risk associated with the Web Printing System and its use of PII.

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

[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).

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

As part of its operations, the Departmental Office of Human Resource Management (DOHRM) is responsible for managing the personal information of all DOT Federal personnel. DOHRM often obtains this personal information from the Department of the Interior's (DOI) Federal Personnel Payroll Systems (FPPS). This personal information is specifically limited to the information collected on the Office of Personnel Management's Standard Forms 50 and 52 (SF-50, Notification of Personnel Action, and SF-52, Request for Personnel Action, respectively).

WPS facilitates the printing of information from FPPS; it does not directly collect information. DOI owns the data in in FPPS and prepopulates the Human Resources (HR) data within the SF-50 and SF 52 forms. It is a secure web-based application owned by the DOT and is designed to allow for data securely auto-transferred by the DOI FPPS to be reviewed and printed for the following:

Personnel Actions (Standard Form-50)
The OPM SF-50 is used to notify and document long term employment events that affect pay and position. The form may include but not limited to full name, social security, date of birth, and pay grade, position information.

Personnel Action Requests (Standard Form-52)
The OPM SF-52 is used to request position and employee actions such as reclassification, new positions, promotion, and appointment. The form may include but not limited to full name, social security, date of birth, and pay grade, position information.

Web Printing uses the information it receives from DOI FPPS to automatically populate the SF Form 50, Notification of Personnel Action, and SF Form 52, Request for Personnel Action. These two standard forms are used by HR specialists when a DOT employee's status of employment changes, such as a hiring, firing, pay increase, grade increase, reassignment, or any other administrative-type action that would require a formal change in the employee's official HR file.

WPS allows DOT personnel to direct user form requests initiated within FPPS to WPS where these forms are programmatically translated into human-readable and printable formats. DOT users can then log into WPS and review these translated forms in their browser. From there, the user can either download the files as PDF and/or print hardcopies to any printer accessible through the users' respective local area network (LAN).

DOT's Web Printing interfaces with the DOI FPPS and has a Memorandum of Understanding (MOU) in place to ensure that each agency's security and privacy standards are equally stringent.

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.

[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

PII is not collected directly from the individual in the system. DOI collects the data and is the data steward. DOI shares information with WPS in accordance with the requirements of the Privacy Act of 1974. Records may be retrieved from DOI FPPS by SSN, name or other unique identifier. The DOT and DOI provides transparency about privacy practices regarding the collection, use, sharing and safeguarding, maintenance, and disposal of information about individuals under the Privacy Act of 1974. Notice is provided to individuals through DOI Privacy Act System of Records Notice is INTERIOR/DOI-85, Payroll, Attendance, Retirement, and Leave Records, 83 FR 34156 (July 19, 2018). There are no exemptions claimed for this system. This SORN is available on the DOI Privacy website and listed under DOI's Wide Systems of Records Notices. PII collected and shared with individuals is only maintained for a short period and removed from the system in accordance National Achieves Records Administration (NARA) records retention requirements.

The Standard forms OPM SF-50 and OPM SF-52 are provided to users for review and printing provides direct notice to individuals on each form. This PIA serves as notice to any members of the public, in this case retired or former DOT Federal employees, whose information may be contained in the system.

Individual Participation and Redress

DOT provides a reasonable opportunity and capability for individuals to make informed decisions about the collection, use, and disclosure of their PII. As required by the Privacy Act, individuals should be active participants in the decision-making process regarding the collection and use of their PII and they are provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

PII on current or former DOT federal employees is contained in WPS. Current Federal employees are responsible for contacting their HR representative to have their data corrected. WPS does not provide immediate notice or collect consent from individuals whose data are contained in the system.

Former and retired individuals wishing to know if their records appear or requiring a request for correction in a system of records may do so in writing with a signed request to:

DOT Chief Privacy Officer
Department of Transportation
1200 New Jersey Ave S.E.
E31-312
Washington D.C. 20590
Email: privacy@dot.gov

Individuals should include in their request the following information:

• Name of DOT Operating Administration (OA) or Division from which you are requesting the search.

• Name of individual

• Mailing address

• Phone number or email address; and

• Description of the records sought, and if possible, location of records.

OR

To the System Manager as stated in DOI SORN, *INTERIOR/DOI–85, Payroll, Attendance, Retirement, and Leave, Records, July 19, 2018, 83 FR 34156, a*s stated in "Notification Procedures". An individual requesting notification of the existence of records on himself or herself should send a signed, written inquiry to the applicable System Manager as identified in DOI 85 SORN. The request must include the requester's bureau and office affiliation to facilitate location of the applicable records. The request envelope and letter should both be clearly marked ''PRIVACY ACT INQUIRY.'' A request for notification must meet the requirements of 43 CFR 2.235.

Individuals wishing to contest information about themselves that is contained in this system should make their request 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 below:

DOT Chief Privacy Officer
Department of Transportation
1200 New Jersey Ave, SE
E31-312
Washington DC, 20590
Email: privacy@dot.gov
Fax: (202) 366-7024

OR

To the System Manager as stated in DOI SORN, *INTERIOR/DOI–85, Payroll, Attendance, Retirement, and Leave, Records, July 19, 2018, 83 FR 34156,* as stated in "Records Access Procedures". An individual requesting records on himself or herself should send a signed, written inquiry to the applicable System Manager identified above. The request must include the requester's bureau and office affiliation to facilitate location of the applicable records. The request envelope and letter should both be clearly marked ''PRIVACY ACT REQUEST FOR ACCESS.'' A request for access must meet the requirements of 43 CFR 2.238."

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.

WPS authority to collect and share PII in this system is covered under 31 U.S.C. 3512, Executive agency accounting and other financial management reports and plan; 5 U.S.C. 1302, Regulations; 5 U.S.C. 2951, Reports to the Office of Personnel Management; 5 U.S.C. 3301, Civil service; generally**;** 5 U.S.C**.** 3372, General provisions; 5 U.S.C. 4118, Government Organizations and Employees; U.S.C. 8506, Dissemination of information; 5 U.S.C. 8347, Administration; regulations; Executive Order (E.O.) 9397,(SSN), as amended.

This system allows DOT personnel to direct user form requests initiated within Federal FPPS to WPS where these forms are programmatically translated into human-readable and printable formats. DOT users can then log into WPS and review these translated forms in their browser.

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 WPS provides PII that is used to populate the requested form(s). It does not permanently store any information. The system does maintain the blank form templates.

When a particular form is required, the information is obtained from DOI FPPS only for the purpose of populating the form. The data copy is purged from WPS after a few days.

Data provided within WPS is retained and disposed of in compliance with the National Archives and Records Administration, General Records Schedules, National Archives and Records Administration. The following schedule(s) apply:

- GRS 4.2, Information Access and Protection Records, *Personally Identifiable Information extract logs. Item 140,* DAA-GRS-2013- 0007-001, Temporary. Destroy when business use ceases.
- GRS 5.2 Transitory and Intermediary Records, Item 10, DAA-GRS 2022-0009-0001, Temporary. Destroy when no longer needed for business use, or according to an agency predetermined time period or business rule.
- *GRS 5.2,* Transitory and Intermediary Records Item 020, DAA-GRS-2022-0009-0002. Disposition: Temporary. Destroy upon creation or update of the final record, or when no longer needed for business use, whichever is later.

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 minimum necessary data is collected and used to ensure compliance with regulations and agency mission. The PII retrieved from the DOI FPPS and populated in the WPS is solely used to populate the requested form(s) SF 50 and SF 52. This information is only collected and shared with individuals who submit a request and for the purposes outlined in this PIA. Only DOT authorized personnel handle the SF 50 and SF 52 form requests. WPS retains and disposes of information it collects in accordance with NARAs approved records retention and disposition. The minimum PII is collected, retrieved, and used to process these requests.

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 WPS relies on the integrity and quality checks from the DOI FPPS system and its Human Resource staff. Individual users and administrators of WPS can only view and print information. It is not and cannot be altered by DOT employees in any way. DOT HR specialists can only view, print these standard forms, and cannot modify them in any way.

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.

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. 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 WPS has a Continuous Monitoring Assessment (CMA) process that supports reaccreditation/reauthorization of the system. The 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.
- WPS 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.

WPS 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. The 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 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. WPS 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.

This system implements a continuous monitoring strategy that includes a configuration management process that determines the security impact of changes to the system and its environment, conducts ongoing assessments, and reports the state of system to organizational officials. An independent assessment team is used to monitor the security controls in the information system on an ongoing basis.

The system maintains an auditing function that tracks all user activities in relation to data including access and modification. Technical security controls include firewalls, intrusion detection, encryption, access control list, and other security methods. Department personnel and contractors supporting the system are required to attend security and privacy awareness training and role-based training offered by the Department. No access is allowed to WPS

prior to receiving the necessary clearances and security and privacy training as required by the Department. All users at the federal level are made aware of the Rules of Behavior (ROB) for IT Systems and accept them prior to being allowed access.

Responsible Official

Stacey McDaniel
Associate Director, HR Systems, OST M-12
Email: stacy.mcdaniel@dot.gov
Phone Number: (202) 366-3314

Approval and Signature

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

KARYN MARIE GORMAN
Digitally signed by KARYN MARIE GORMAN
Date: 2024.11.05 09:31:08 -05'00'