Privacy Impact Assessment for

Workforce Reshaping Tool (WRT)

April 30, 2025

Contact Point
Caleb Judy
Program Manager
Human Resources Solutions

Reviewing Official
Becky Ronayne
Acting Senior Agency Official for Privacy

Abstract

OPM is responsible for providing guidance and assistance to federal agencies that are considering and/or undergoing efforts to reshape their organizations, including through reduction in force (RIF) activities. The RIF process requires strict adherence to merit system laws and regulations. The WRT is designed to guide agencies through the RIF process, ease the administrative burden of conducing RIF activities, and help ensure RIF actions are conducted consistently with applicable law and regulations. This PIA is being completed because WRT is a new system that uses PII from employees to calculate their retention standing in RIF activities.

Overview

When federal agencies go through a Reduction in Force (RIF), 5 CFR Part 351, Reduction in Force, defines how the agency determines which employees retain their current position or have a right to a different position. The determinations are based on several factors including each employee's type of appointment, tenure, veterans' preference, length of service, and performance ratings. Further information about RIFs is available at https://www.opm.gov/policy-data-oversight/workforce-restructuring/reductions-in-force-rif/.

WRT is an OPM-developed application that helps agencies manage the RIF process. An approved user can authenticate into the WRT website, upload personally identifiable information (PII) about a set of employees, proceed through all rounds of the RIF competition, and produce retention registers. WRT is structured around a fixed set of business rules which match the requirements in 5 CFR Part 351. The user can then save the results to their local machine or network to resume the session later and for reporting and audit purposes.

WRT uses a client-side data architecture where the employee information uploaded by a user, and all the processing, are done within the user's

browser. No information in WRT is ever transferred to an OPM database or server (except WRT records for OPM employees). Users who want to keep their work must save it to their local machine or network. Users who want to continue a prior project must upload their information back into WRT. Each agency owns and manages the information uploaded and generated by WRT.

OPM intends to use WRT for its own RIF activities and when hired to support other agency's RIF activities through interagency agreements (called "customer agencies"). OPM also intends to share WRT with other agencies so they can independently use it to conduct their own RIF activities. While this PIA will discuss all three cases, other federal agencies may choose to develop their own PIA to assess their own use of the tool.

Section 1.0. Authorities and Other Requirements

1.1. What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

WRT is used to guide agencies through the RIF competition process. Agency RIF procedures that require the collection and use of federal employee PII are detailed in 5 U.S.C. 1302, 5 U.S.C. 3502, 5 U.S.C. 3503, and 5 CFR Part 351.

1.2. What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The SORNs that apply to the records when OPM uses WRT for its own RIF activities are OPM/GOVT-1, General Personnel Records, and OPM/GOVT-2, Employee Performance File System Records. Other agencies using WRT may choose to use records covered by additional or different SORNs.

1.3. Has a system security plan been completed for the information system(s) supporting the project?

WRT operates in the USADATA FISMA system. USADATA obtained an Authority to Operate (ATO) on November 13, 2024. A system security plan was completed as part of the ATO package.

1.4. Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

WRT does not retain, save, or store any records. It uses a client-side data storage architecture, so all PII used in WRT stays in the browser of the user. The General Records Schedule for information on agency separation initiatives such as a RIF is General Records Schedule 2.5, Item 011 - Separation program management records.

1.5. If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

WRT does not collect information directly from individuals, so it is not covered by the Paperwork Reduction Act.

Section 2.0. Characterization of the Information

2.1. Identify the information the project collects, uses, disseminates, or maintains.

Users upload the following information into WRT about the employees who are part of a RIF: employee ID, position ID, position status, employee first name, employee middle name, employee last name, position title, competitive level code, pay plan, series, grade, step, salary, position occupied, tenure group, veterans preference, RIF service computation date, position description number, work schedule, appointing authority, annuitant indicator, security clearance level, supervisory status, competitive area, organization code, organization description, sub organization code, sub

organization description, duty location code, duty location description, performance ratings, and performance rating dates.

2.2. What are the sources of the information and how is the information collected for the project?

When OPM uses WRT for its own RIF activities, the records will come from the individual's Electronic Official Personnel Folder (eOPF). OPM and many other agencies store this data in a talent management system (covered by OPM/GOVT-1) and a performance management system (covered by OPM/GOVT-2). OPM uses USA Performance as its performance management system and HRLinks as its core human resources system. OPM and other agencies will extract the information from those systems, format it according to the WRT guidance, then upload it into WRT.

2.3. Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No, WRT does not use any commercial or publicly available data.

2.4. Discuss how accuracy of the data is ensured.

OPM and all other federal agencies undergoing RIF procedures undertake a rigorous process to ensure employee data from source systems are correct and validated prior to initiating a RIF competition. WRT includes documentation and a file upload template to help ensure users upload accurate and correctly formatted data into the system. OPM rigorously tests the WRT system to assure it produces a RIF retention registry matching the requirements set in 5 CFR Part 351. Additionally, WRT users are encouraged to go through multiple rounds of the RIF process (manually and/or using a system like WRT) to ensure the data is accurate.

2.5. Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that PII used in WRT is inaccurate and will result in inaccurate RIF results.

Mitigation: OPM and all other agencies undergoing RIF procedures go through a rigorous data validation process to ensure the information used for that process is accurate. In the Rules of Behavior for the system, WRT users assure their agency has reasonably verified the accuracy of PII uploaded into WRT. WRT includes validation rules to ensure PII is properly formatted and has conducted rigorous testing to ensure the business rules of the system adhere to applicable laws and regulation.

Section 3.0. Uses of the Information

3.1. Describe how and why the project uses the information.

The RIF process requires strict adherence to merit system laws and regulations (e.g., 5 CFR Part 351). This includes a complex calculation on who is retained based on several factors including type of appointment, tenure, veterans' preference, length of service, and performance ratings. WRT is designed to guide agencies through the RIF calculations, ease the administrative burden of conducing RIF activities, and help ensure RIF actions are conducted consistent with applicable law and regulations.

An approved WRT user can authenticate into the WRT website, upload the PII described in section 2.1 about a set of employees, proceed through all rounds of the RIF competition, and produce retention registers. The user can then save that information to their local machine or network so that it can be used to help execute the RIF and then stored for reporting, auditing, and related purposes.

3.2. Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how OPM plans to use such results.

No. WRT does not use any artificial intelligence or technology to conduct electronic searches, queries, or analyses to discover or locate a predictive

pattern. Moreover, WRT is structured around a fixed set of business rules which match the requirements in 5 CFR Part 351.

3.3. Are there other programs or offices with assigned roles and responsibilities within the system?

OPM OCIO and Human Resources Solutions (HRS) staff have assigned roles and responsibilities within the system to develop and maintain WRT. WRT does not store PII, so these staff do not have access to PII in the WRT system.

OPM OCHCO will be responsible for using WRT to carry out its own RIF activities and OPM HRS will be responsible for using WRT when hired by customer agencies.

3.4. Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that unauthorized individuals may access the PII in WRT and use it for an unauthorized purpose, or that authorized users will access and use the PII for unauthorized purposes.

Mitigation: OPM will use another system called USADATA to control who can access WRT. OPM and other agencies interested in using WRT will need to contact the USADATA team and specify which individuals need access to WRT to help with RIF calculations. That should greatly reduce the risk that individuals access WRT and use it for an unauthorized purpose.

WRT information is not centrally-stored within the application; all information resides with the user. Moreover, all WRT users must sign a Rules of Behavior document which states how they will protect the information created through WRT. That should greatly reduce the risk that authorized users will access and use the information in WRT for an unauthorized purpose.

Section 4.0. Notice

4.1. How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

None of the information collected into WRT will come directly from individuals so there will not be an opportunity to provide notice to individuals at the point it is collected into WRT. However, when the information was originally collected from the individuals, the Federal agencies and systems that collected the information were required to notify the individuals that their information would be used for employment-related purposes via Privacy Act Statements and other documentation.

4.2. What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

The Federal agencies and systems that originally collected the data that will be used in WRT were responsible for giving individuals the option to consent, decline, or opt-out as permitted by applicable law and regulation. In general, several employment regulations require federal agencies to collect the employment information that will be used in WRT and additional regulations give federal agencies the authority to conduct RIFs.

4.3. Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals have not received adequate notice concerning why their PII is being collected and how it will be used.

Mitigation: All federal agencies are required to keep Privacy Act Statements and notices on relevant forms and collections of information current and accurate.

Section 5.0. Data Retention by the Project

5.1. Explain how long and for what reason the information is retained.

WRT does not retain data. WRT does allow users to export the data so it can be stored. Maintaining RIF-related records, including those created with WRT, is the responsibility of the federal agency carrying out the RIF.

The records created by WRT fit General Records Schedule 2.5, Item 011 - Separation program management records: ***Temporary.*** *Destroy 2 years after date of program closure, but longer retention is authorized if required for business use.*

5.2. Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that the PII in WRT will be retained for longer than is necessary to fulfill the business need for the information.

Mitigation: WRT does not retain PII. Agencies using WRT are responsible for following applicable records schedules.

Section 6.0. Information Sharing

6.1. Is information shared outside of OPM as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

When OPM uses WRT for its own RIF activities, OPM may later share that information for reporting, auditing, and related purposes when permitted by the appropriate SORN.

When OPM uses WRT to support other agency's RIF activities, agencies share the information WRT requires with OPM, and OPM returns the WRT RIF session files and retention registers to those agencies for their use and management.

OPM provides a mechanism for Federal agencies to use WRT and their own information to conduct their own RIF processes and share accordingly. This responsibility will likely be given to the agency's human resources office.

6.2. Describe how the external sharing noted in 6.1 is compatible with the SORNs noted in 1.2.

When OPM uses WRT for its own RIF activities, any external sharing of the information will match what is permitted under OPM/GOVT-1 or OPM/GOVT-2, depending on the records being shared.

When OPM uses WRT to support other agency's RIF activities, the customer agency will instruct OPM where OPM can share the information in the interagency agreement.

When other federal agencies use WRT for its own RIF activities, those agencies will determine how they share employee information and RIF session files outside the agency.

6.3. Does the project place limitations on re-dissemination?

OPM and all other federal agencies are subject to the applicable SORNs and are constrained in their re-dissemination of information based on their terms.

When OPM uses WRT to support other agency's RIF activities, the customer agency will instruct OPM where OPM can re-disclose the information in the interagency agreement.

All WRT users will also sign a Rules of Behavior document which discusses the need to protect the data used in WRT and says they may only disclose it for authorized purposes in accordance with established regulations and procedures.

6.4. Describe how the project maintains a record of any disclosures outside of OPM.

WRT data is not centrally stored. Data is housed at each Federal agency using WRT. WRT does share or maintain PII so any sharing will need to occur outside the system, and any record of that sharing will need to be maintained outside the system.

6.5. Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information will be disclosed and used for a purpose that is not consistent with the business purpose for which the information was initially collected.

Mitigation: This risk is mitigated through the client-side data architecture. All agency users are subject to the SORN referenced in Section 1.2 and are constrained in their re-dissemination of information based on those terms.

Section 7.0. Redress

7.1. What are the procedures that allow individuals to access their information?

OPM, and all other employees, can contact their supervisor or human resources office to access their employee information. OPM and several other agencies may also have various systems where employees can login and review their own information.

The SORNs describing the systems where the information used in WRT is acquired and then stored also include processes by which individuals may access their own records within those systems.

7.2. What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

OPM, and all other employees, can contact their supervisor or human resources office to request a correction to their employee information. OPM

and several other agencies may also have various systems where employees can login to review and request changes to their own information.

The SORNs describing the systems where the information used in WRT is acquired and then stored also include processes by which individuals may request updates to their own records if inaccurate.

There are also several processes in place for individuals who believe the information used to calculate their RIF or the outcome were incorrect.

7.3. How does the project notify individuals about the procedures for correcting their information?

Federal employees can find the procedures in the SORNs identified in Section 1.2. or by contacting their supervisor or human resources office.

7.4. Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals will not be knowledgeable about how to access or correct their information.

Mitigation: Federal employees should know to contact their supervisor or human resources office to correct erroneous human resources related information. Each SORN has a process for individuals to follow to correct information.

Section 8.0. Auditing and Accountability

8.1. How does the project ensure that the information is used in accordance with stated practices in the PIA?

Only users authenticated and authorized through USADATA will be able to access WRT. All these individuals will be informed how they may and may not use the PII uploaded and downloaded from WRT.

With the client-side data architecture, Federal agencies using WRT are ultimately responsible for ensuring they are using their data consistent with the stated practices in the PIA.

The WRT code is stored in USADATA, and any code changes go through a standard release process.

8.2. Describe what privacy training is provided to users either generally or specifically relevant to the project.

All OPM employees are required to take annual IT Security and Privacy Awareness Training, while employees in other agencies are expected to complete their own security and privacy trainings.

Individuals who access WRT will sign a rules of behavior document before they access the system and can download guidance on how to use WRT from within the tool.

8.3. What procedures are in place to determine which users may access the information and how does the project determine who has access?

Each federal agency customer determines which individuals within their organization will be an authorized user of WRT and assumes responsibility for ensuring that they choose the appropriate agency users. System access to WRT is provided on an annual basis. Only authenticated and authorized users may obtain access to WRT.

8.4. How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within OPM and outside?

When customer agencies hire OPM to support their RIF activities, both agencies sign an interagency agreement which establishes how OPM will use the data shared by that organization.

All users, including users from agencies independently using WRT to conduct their own RIF activities, must electronically sign the Rules of Behavior for WRT.

Any new uses of the information or information-sharing agreements will be evaluated by the USADATA program in consultation with the federal agencies and appropriate OPM stakeholders, including the Office of the General Counsel, the Chief Privacy Officer, and the Chief Information Security Officer.

Responsible Officials

Caleb Judy
Program Manager
Human Resources Solutions

Approval Signature

Signed copy on file with Senior Agency Official for Privacy

Becky Ronayne
Acting Senior Agency Official for Privacy