



Privacy Impact Assessment for
Electronic Official Personnel Folder System
(eOPF)

October 28, 2020

Contact Points

System Owner Point of Contact

Rhonda Wood

Program Manager

Human Resources Solutions Information Technology Program
Management Office (HRSITPMO)

Business Owner Point of Contact

Victor A. Karcher, Jr.

eOPF Program Director

Human Capital Data Management & Modernization (HCDMM)

Reviewing Official

Kellie Cosgrove Riley, Chief Privacy Officer



Abstract

The electronic Official Personnel Folder system (eOPF) maintains the official digital imaged versions of the Official Personnel Folders (OPF) for Federal employees and contains various work folders used by human resource offices. It also maintains records for non-Federal employees managed by Federal agencies. This privacy impact assessment is being conducted because eOPF contains sensitive personally identifiable information about individuals.

Overview

Each Federal employee has a single personnel folder, known as the OPF, which documents the entire period of Federal civilian service. The eOPF system contains an electronic version (digital images) of the paper OPF for Federal employees, virtual work folders for use by human resource (HR) offices, and folders for non-federal employees that are accessible online. The OPF (Standard Form 66) is a file containing records from an individual's federal employment career. Employees with OPFs are those in the Executive Branch service, as listed in Title V of the United States Code, and some federal employees not under Title V. The long-term records in the file are included to protect the legal and financial rights of the government and the employee.

The OPF contains records the Government needs to make accurate employment decisions throughout an individual's Federal career. Some of these records show that a Federal appointment was valid (e.g., the Appointment Affidavit and the Declaration for Federal Employment), or verify military service credit for leave, reduction-in-force, or retirement (e.g., the DD 214, Certificate of Release or Discharge from Active Duty, and the Military Service Deposit Election). The records also establish an individual's employment history, grades, occupations, and pay (e.g., Standard Form 50, Notification of Personnel Action), and document choices



made by the Federal employee under Federal benefits programs (e.g., the Health Benefits Registration Form and the Designation of Beneficiary under the Federal Employees' Group Life Insurance Program).

The e-GOV initiative of the President's Management Agenda initiated in July 2001 challenged the Federal government to automate where it makes sense. The Office of Management and Budget (OMB) was charged with the implementation to reduce the amount of paper used by automating business processes. The Office of Personnel Management (OPM), working with the OMB, advised agencies that they had to convert the OPFs of their employees to an electronic format. eOPF is the solution that OPM chose for the Federal government.

The eOPF system combines document management with workflow capabilities, provides immediate access to personnel forms and information for a geographically dispersed workforce, and sends email notifications to employees when documents are added to their electronic folders. Added benefits of the system are the reduced costs associated with storage, maintenance, and retrieval of records, as well as integration with the agency's human resources information systems. The system also allows for compliance with OPM and federally mandated HR employee record management regulations.

The same personally identifiable information (PII) that is contained in a paper OPF is contained in its electronic version and it is accessed via the Internet using a login ID and password or Personal Identity Verification (PIV) card credentials. Users are defined by their roles, which includes employee, agency HR Specialist, investigator, and agency administrator. For example, when an employee logs into eOPF, he or she is limited to read only access of his or her individual Permanent and Temporary folders and cannot access or view any other employee folders. The Permanent and Temporary folders are the electronic equivalent to the employee's paper OPF and employees cannot modify the documents. Similarly, the HR Specialist access is limited to the Permanent and Temporary folders and HR work folders of employees to



whom they provide HR services. Each agency establishes HR work folders based on agency needs and the folders include but are not limited to folders for performance, payroll, staffing, security and benefits. The system stores each agency's data separately and maintains continuous segregation of information.

Government officials who need to see the records in eOPF to do their jobs are also given access. For example, Investigators are granted access to the employee folders they are assigned to investigate. eOPF includes an audit trail that records when and why an individual reviewed a folder within the eOPF system.

The eOPF system owner is the OPM Office of the Chief Information Officer, Human Resources Solution IT Program Management Office (HRS IT PMO) and resides in Macon, Georgia. The eOPF business owner is the Human Capital Data Management and Modernization's (HCDMM) eOPF Program Office located in Washington DC. eOPF is funded through interagency agreements with the eOPF participating agencies on a fiscal year basis and is administered through the OPM revolving fund.

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?

5 CFR 293.302 created the OPF to house paper records used by Federal government HR offices. These records establish an employment history that includes grades, occupations and pay, and records choices under Federal benefits programs and were maintained as paper in agency HR offices until they were converted to digital images as part of an e-Government initiative established in response to the E-Government Act of 2002.

In general, OPM collects and maintains the information in eOPF pursuant to 5 U.S.C. §§ 1104, 1302, 2951, 3301, and 4315; E.O. 12107 (December 28,



1978), 3 CFR 1954-1958 Comp.; 5 U.S.C. 1104, and 1302; 5 CFR 7.2; Executive Orders 9830 and 12107; 3 CFR 1943-1948 Comp.; and 5 U.S.C. 2951(2) and 3301 authorize the maintenance of records the Government needs to make accurate employment decisions throughout an employee's career. 5 CFR Chapter 1 part 293 Personnel Records.

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

The OPM/GOVT 1, General Personnel Records; OPM/GOVT 2, Employee Performance File System; and, OPM/GOVT 3, Records of Adverse Actions, Performance Based Reduction in Grade and Removal Actions, and Termination of Probationers SORNs apply to the information maintained in eOPF about Federal employees. Individual agencies who have records in eOPF that do not fall within the purview of the previously listed Government-wide SORNs have their own applicable SORNs. For example, the USDA/FSA 6, County Personnel Records, and USDA/OP-1, Personnel and Payroll System SORNs apply to the information maintained on non-Federal county employees for USDA.

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

Yes, the Authority to Operate (ATO) for eOPF was granted on July 8, 2019. The system security plan is part of the ATO package.

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

Yes, GRS 2.2, Item 040 (DAA-GRS-2017-0007-0004) covers the eOPF records and requires that they be destroyed when survivor or retirement claims are adjudicated or when records are 129 years old, whichever is sooner, but longer retention is authorized if required for business use. In addition, each agency establishes a records retention schedule for the virtual work folders maintained by their organization in eOPF. The agencies that manage non-Federal employees establish records retention schedules for the records they maintain on those individuals in eOPF.



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.

The PRA does not apply directly to the eOPF system. Numerous forms that are ultimately placed in the eOPF, however, are subject to the PRA. While the eOPF is the repository for the forms, the program does not manage or regulate the collection of the information on the forms. The complete listing of forms in eOPF can be found on the Master forms list at <https://www.opm.gov/policy-data-oversight/data-analysis-documentation/enterprise-human-resources-integration/MasterFormsList/Permanent/index.aspx>.

Section 2.0. Characterization of the Information

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

The system collects, uses, disseminates and maintains information about individuals and their Federal employment. This information typically includes employee's full name, date of birth (DOB), Social Security number (SSN), mailing address, home address, email address, telephone numbers, military service id, health and/or life insurance policy numbers, SSN of family members, DOB of family members, address of family members, bank account number, certificate/license number, civil or criminal history information, education record and other identifying information. In addition eOPF may contain information about past and present positions held; grades; salaries; duty station locations; notices of all personnel actions, such as appointments, transfers, reassignments, details, promotions, demotions, reductions-in-force, resignations, separations, suspensions, OPM approval of disability retirement applications, retirement, and removals; work experience; education level; specialized education or training obtained outside of Federal service; agency specific forms; and other documents



relating to the recruitment, service history, payroll, benefits, retirement, performance and security clearance of an employee. For members of the Senior Executive Service, eOPF may include information relating to sabbatical leave programs, reassignments, and details.

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

Federal agencies submit forms to eOPF for filing in an employee's eOPF or a virtual work folder. The most common forms are the Oath of Office, health benefits registration and changes, life insurance registration and changes, resume, position description, employment eligibility verification, security clearance approval, designation of beneficiaries, Thrift Savings Plan election and changes, veteran's preference designation and verification, and personnel actions.

The information on the forms is completed by the individual or an agency's HR specialists electronically in an agency sponsored system or on paper which is then entered into the agency sponsored system by HR. These agency sponsored systems may be developed and owned by the agency or by another agency that provides HR and or payroll services to other agencies. The provider of the HR and payroll services sends the information to the eOPF system as a PDF or as data that is then placed on a template by eOPF to create a PDF.

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, eOPF does not use information from commercial sources or publicly available data.

2.4. Discuss how accuracy of the data is ensured.

It is the responsibility of the agency or data provider collecting the data to ensure its accuracy and relevance before submitting it to eOPF. eOPF does not validate the data submitted by the agencies and providers.



Agencies are also responsible for correcting errors in the data by following specific policy and guidance described in the Guide to Processing Personnel Actions (GPPA). The GPPA is available for viewing/printing on the OPM web site <https://www.opm.gov/policy-data-oversight/data-analysis-documentation/personnel-documentation/#url=Processing-Personnel-Actions>.

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

Privacy Risk: There is a risk that the information in eOPF is not accurate or is filed incorrectly and, as such, will result in incorrect personnel decisions or benefit calculations.

Mitigation: This risk is mitigated by the agencies who submit information to eOPF, which are required to determine that it is accurate, complete, and filed correctly, based on the GPPA and Guide to Personnel Recordkeeping (GPR) guidance. The GPPA contains OPM's instructions on how to prepare personnel actions. The GPR describes general policies governing the creation, maintenance, and disposition of records used to document HR management programs established by OPM. In addition, in the event agency employees find documents in eOPF that do not belong to them, OPM has issued FAQs and other instructions so corrective measures can be taken.

Privacy Risk: There is a risk that the information collected in the eOPF is not personnel information about Federal employees and will not be used, retained, and disseminated properly.

Mitigation: OPM is mitigating this risk by working with each agency that maintains non-Federal employee data in eOPF to determine that the agencies have appropriate measures in place concerning use, retention, and dissemination of information about non-Federal employees.



Section 3.0. Uses of the Information

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

eOPF aggregates and maintains career lifecycle information and form images for current, separated, and retired Federal employees and non-Federal employees managed by Federal agencies. The information is viewable through a secure user interface. Information in eOPF is indexed/filed using the SSN in combination with the employee's full name and date of birth to validate the employee's identity and assure correct filing of documents.

The project uses the information to enhance the HR workflow capabilities. eOPF allows each employee to have a dedicated electronic personnel folder instead of a paper folder. This provides individuals with immediate access to their personnel forms and information, and notification of changes to their OPF.

The information in eOPF is used by Federal agencies to make employment decisions throughout an employee's career. The information is used for personnel-related determinations, such as demonstrating that the appointment to federal services was valid; to verify military service credit for leave, reduction-in-force, or retirement; to establish an employment history, including grades, occupations and pay; and to document the choices an employee has made with respect to Federal benefits programs, including designating beneficiaries and selecting a health insurance carrier.

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, the eOPF system does not use technology to conduct electronic searches, queries, or analysis to discover or locate a predictive pattern or an anomaly.



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

There are other OPM offices and programs with assigned roles and responsibilities within the eOPF system. For example, OPM HR Specialists have read-write access to employees' eOPFs within their service area and OPM investigators have access to relevant records when conducting a background investigation. eOPF employs role-based access controls, which categorize users and permit access according to their role. The other OPM offices with authority to access OPFs include:

Retirement Services (RS): OPM Retirement Adjudicators processing retirement cases access the folders of retiring employees to verify service and benefits eligibility.

Merit System Audit & Compliance (MSAC): MSAC conducts HR evaluations examining a broad range of HR programs, including staffing and competitive hiring, performance management, and leadership and succession planning. MSAC evaluators access a sample of OPFs to review employment history, educational degrees, and military services to name a few. The evaluators send advance information requests (usually via email) to the agency HR point of contact to specify the selected employees OPFs included in the sample.

OPM and Agency Support: OPM Support consists of HCDMM, eOPF Program staff and contractors, HRSITPMO (Macon Data Center) Systems Capacity Branch, OPM HRS IT PMO (Macon Data Center) Employee Systems Branch, OPM HRS IT PMO Software Quality Assurance Branch, OPM Chief Information Security Officer, OPM Enterprise Information Services, and OPM Office of Inspector General personnel.

OPM Data Management: HCDMM, which requires access when an eOPF record must be amended pursuant to the Privacy Act.



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

Privacy Risk: There is a risk that unauthorized users may access the information in the eOPF and use it for purposes that are inconsistent with the personnel purposes for which it was collected.

Mitigation: This risk is mitigated through the use of role-based access controls, which only permit designated individuals to access information they need to know to perform their job responsibilities.

Privacy Risk: There is a risk that authorized users may access information that they are not authorized to see or use information for an unauthorized purpose such as performing searches on themselves, friends, relatives, or neighbors. Also, authorized users may inappropriately disclose this information, either intentionally or unintentionally.

Mitigation: This risk is mitigated through the use of role-based access controls, which limit the information authorized users can access to that which they need to know. In addition, OPM conducts periodic security audits, regularly monitors security practices, and requires users to agree to rules of behavior to indicate they understand and will adhere to appropriate data use.

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.

Individuals who seek to access eOPF to view their own personnel records are able to review the eOPF Privacy Policy, which addresses the collection and use of information. In addition, individuals are provided with notice through Privacy Act statements on the various forms that ultimately become a part of their eOPF.

Notice concerning the collection and use of the information in eOPF is also provided via the SORNs listed in question 1.2 and through this PIA.



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 using eOPF determine what information is sent to the system and there is no ability to consent to particular uses of information in eOPF or for individuals to decline to have their information included in the system.

4.3. Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals may not be aware that their information will be placed in the eOPF and accessed and used for various personnel reasons.

Mitigation: This risk is mitigated through the use of Privacy Act statements on various agency forms that inform individuals concerning why and for what purpose their information is being collected. In addition, individuals are provide notice concerning eOPF through the Privacy Policy they are presented with when accessing their records and concerning the collection and use of their information via the SORNs referenced in Section 1.2 and this PIA.

Section 5.0. Data Retention by the Project

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

When an employee leaves an agency, the OPF is transferred to either the National Personnel Records Center (NPRC) or the employee's new agency. The losing agency purges the OPF and work folders in eOPF and, at that point, the employee and the agency personnel no longer have access to the records. The new agency grants access to the employee and appropriate HR specialists, Investigators and system administrators.

The electronic versions of the OPFs for Federal employees who do not continue in Federal service with another agency are maintained in the eOPF



system in an area managed by NPRC. NPRC is one of the National Archives and Records Administration's (NARA) largest operations and is the central repository of personnel-related records for both the military and civil services of the United States Government.

The records are retained pursuant to the records schedule identified in Section 1.4.

5.2. Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that the information in eOPF will be retained longer than is necessary for its intended business purpose.

Mitigation: This risk is mitigated by requiring adherence to the appropriate records retention schedule and by providing guidance to eOPF users in the OPM GPR, which describes general policies governing the creation, maintenance, and disposition of records used to document HR management programs established by OPM. OPM cannot enforce the adherence to policy or the retention schedule practices at other agencies. However, NARA guidance does dictate compliance.

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.

As part of the normal agency operations, eOPF data is generally not shared with organizations other than to those agencies that provided the collected data. The information in the eOPF system is used by Federal agency HR offices to make employment decisions throughout an employee's career. In addition, the information in the eOPF may be shared for background investigation purposes with Defense Counterintelligence and Security Agency (DCSA) investigators, who access eOPF to perform work during investigations processing such as initial background checks and renewal of



existing investigations. DCSA is not authorized to conduct a background investigation unless a release, signed by the subject of the investigation is received.

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

The external sharing described above is consistent with the purposes for which the information was collected, as documented in the applicable SORNS listed in Section 1.2. In general, this includes use for personnel-related determinations, such as demonstrating that the appointment to Federal services was valid; to verify military service credit for leave, reduction-in-force, or retirement; to establish an employment history, including grades, occupations and pay; and the choices an employee has made with respect to Federal benefits programs, including designating beneficiaries and selecting a health insurance carrier.

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

OPM does not explicitly limit the re-dissemination of eOPF information by the agencies. However, those agencies are required to adhere to the government-wide SORNS referenced in Section 1.2 and cannot re-disseminate the information except pursuant to an applicable routine use.

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

The eOPF system contains automated audit log capabilities that record all access and review of the information in the system, as well as the reason for the review. eOPF also manual processes that require documentation, justification and approval of all access, reviews and removal of data that occurs outside the automated audit log functionality.

6.5. Privacy Impact Analysis: Related to Information Sharing

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



Mitigation: This risk is mitigated by provisions in MOUs with participating agencies that require the recipients of the information to use it only for the purpose for which it is provided.

Section 7.0. Redress

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

Individual employees may access their records through an IP allow list and authenticate to eOPF using a login ID and password, e-Authentication/Single Sign-on, or Personal Identity Verification (PIV) card credentials issued by their agency. When an employee logs into eOPF, he or she has read only access only to his or her individual folder

In addition, individuals can submit a Privacy Act request for their records by following the process outlined in the applicable SORNs listed in 1.2.

Individuals requesting access must comply with OPM's Privacy Act regulations on verification of identity and access to records (5 CFR part 297). Current Federal employees should contact the Personnel Officer or other responsible official of their agency. Former Federal employees should contact the National Personnel Records Center (Civilian), 111 Winnebago Street, St. Louis, Missouri 63118.

In general, individuals must furnish the following information for their records to be located and identified:

- Full name(s).
- Date of birth.
- Social security number.
- Last employing agency (including duty station) and approximate date(s) of employment (for former Federal employees).



- Signature.

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

Current Federal employees wishing to request amendment of their records should contact their current agency. Former employees should contact the Office of Personnel Management. Individuals must furnish the following information for their records to be located and identified.

- Full name(s).
- Date of birth.
- Social security number.
- Last employing agency (including duty station) and approximate date(s) of employment (for former Federal employees).
- Signature.

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

Email notifications are sent to employees when documents are added to their eOPF folders. The notifications contain instructions indicating the employee should review the new document(s) and notify their HR office when there is inaccurate or erroneous information. In addition, the SORNs referenced in Section 1.2 provided instructions to individuals who wish to request an amendment to their records.

7.4. Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals will not understand how to access and correct their records in eOPF.

Mitigation: This risk is mitigated through publishing clear instructions on various OPM and agency websites, in the SORNs, and in this PIA informing individuals how to access and request amendment to their records. Further



assistance to gain access or make amendments is given in eOPF within the online FAQs that can be viewed by clicking the word 'FAQ' at the top of the login page within the web site. The instructions in the FAQs can be printed.

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?

eOPF contains automated audit log capabilities that record all access and review of the information contained in the system as well as the reason for the review. All activities performed in the eOPF application are logged and the audit logs are periodically reviewed to ensure that the information is being accessed and used appropriately.

In addition, eOPF includes security features to protect the integrity of user information including requiring agencies to limit access to the minimal level that allows normal functioning.

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

All OPM employees and contractors who support the eOPF system must complete OPM-provided, mandatory, annual Security and Privacy Awareness Training prior to gaining access to eOPF. In addition, OPM offers training to HR Specialists and employees designated as systems administrators specific to the eOPF system. This training stresses the importance of protecting personally identifiable information and teaches the individuals to navigate through eOPF to complete their work assignments.

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

eOPF employs role-based access controls, which categorize users as employee, Investigator, HR Specialist, or agency administrator and permit



access according to their role. The agencies that submit information to eOPF determine which of their HR Specialists require access.

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 an agency elects to use the eOPF system, the OPM security staff works with the agency to enter into an ISA and MOU. These are reviewed by relevant OPM stakeholders and signed by both parties. The ISAs and MOUs are updated every three years or when there are changes to the system.

Responsible Officials

Rhonda Wood
Program Manager
Human Resources Solutions Information
Technology Program Management Office
Office of the Chief Information Officer

Victor A. Karcher, Jr.
Program Director
eOPF Program
Human Capital Data Modernization & Management

Approval Signature

Signed Copy on file with the Chief Privacy Officer

Kellie Cosgrove Riley
Chief Privacy Officer