ADAMS ML18075A265

U.S. Nuclear Regulatory Commission

Privacy Impact Assessment

Designed to collect the information necessary to make relevant determinations regarding the applicability of the Privacy Act, the Paperwork Reduction Act information collection requirements, and records management requirements.

Electronic Official Personnel Folder (eOPF)

Date: March 15, 2018

A. GENERAL SYSTEM INFORMATION

1. Provide a detailed description of the system:

The Electronic Official Personnel Folder (eOPF) is a web-based external system owned by the Office of Personnel Management (OPM). The eOPF stores official personnel files and human resource records related to Federal civilian employees. The system is utilized by the NRC's human resource staff to manage employee electronic personnel records. Employees are able to access their individual Official Personnel Folder (OPF) in eOPF and view the documents, but they cannot modify the documents. No system components are housed on the NRC infrastructure.

2. What agency function does it support?

The eOPF supports the management of human resource management of official personnel files.

3. Describe any modules or subsystems, where relevant, and their functions.

N/A

4. What legal authority authorizes the purchase or development of this system?

The eOPF is an e-government initiative owned by the OPM and mandated by the Office of Management and Budget (OMB).

What law, regulation, or Executive Order authorizes the collection and maintenance of the information necessary to meet an official program mission or goal? NRC internal policy is not a legal authority.

5 CFR 293.302 mandated that each agency shall establish an OPF for each employee 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.

5. What is the purpose of the system and the data to be collected?

The data will be used by HR personnel for human resource functions.

6. **Points of Contact:**

Project Manager	**Office/Division/Branch**	**Telephone**
Brendan Cain	*OCHCO/HCAB*	*301-287-0552*
Technical Project Manager	**Office/Division/Branch**	**Telephone**
Brendan Cain	*OCHCO/HCAB*	*301-287-0552*
Executive Sponsor	**Office/Division/Branch**	**Telephone**
Miriam Cohen	*OCHCO*	*301-287-0747*

7. Does this privacy impact assessment (PIA) support a proposed new system or a proposed modification to an existing system?

a. ___ New System __x__ Modify Existing System ____ Other (Explain)

b. If modifying an existing system, has a PIA been prepared before?

Yes

(1) If yes, provide the date approved and ADAMS accession number.

A PIA was developed January 22, 2009. ML090550710

(2) If yes, provide a summary of modifications to the existing system.

eOPF cybersecurity compliance will be managed under the Third Party System (TPS) and changes have been made to where the system is hosted.

B. INFORMATION COLLECTED AND MAINTAINED

These questions are intended to define the scope of the information requested as well as the reasons for its collection. Section 1 should be completed only if information is being collected about individuals. Section 2 should be completed for information being collected that is not about individuals.

1. INFORMATION ABOUT INDIVIDUALS

a. Does this system maintain information about individuals?

Yes

(1) If yes, identify the group(s) of individuals (e.g., Federal employees, Federal contractors, licensees, general public).

Current and former NRC employees.

(2) **IF NO, SKIP TO QUESTION B.2**.

b. What information is being maintained in the system about an individual (be specific)?

HR data included in eOPF includes notification of personnel action (SF-50) and documents supporting the action taken; life insurance, Thrift Savings Plan, health benefits and related beneficiary forms; letters of disciplinary action; notices of reductions-in-force; and other records retained in accordance with the OPM's Guide to Personnel Recordkeeping.

Records include employment information such as personal qualification statements, resumes, and related documents including information about an individual's birth date, social security number, veterans preference status, tenure, minority group designator, physical handicaps, past and present salaries, grades, position titles; employee locator information identifying home and work address, phone numbers and emergency contacts; and certain medical records related to initial appointment and employment.

c. Is information being collected from the subject individual?

Records maintained in eOPF are collected from the individual and from HR professionals.

(1) If yes, what information is being collected?

Individuals provide resumes, birth date, social security number, veteran preference status, tenure, minority group designator,

physical handicaps, past and present salaries, grades, position titles

d. Will the information be collected from 10 or more individuals who are not Federal employees?

No

(1) If yes, does the information collection have OMB approval?

(a) If yes, indicate the OMB approval number:

e. Is the information being collected from existing NRC files, databases, or systems?

Yes

(1) If yes, identify the files/databases/systems and the information being collected.

eOPF collects existing Official Personnel Folder records.

f. Is the information being collected from external sources (any source outside of the NRC)?

Yes

(1) If yes, identify the source and what type of information is being collected?

eOPF collects information from Federal Personnel/Payroll System (FPPS), Workforce Transformation Tracking System (WTTS) and Employee Express (EEX).

g. How will information not collected directly from the subject individual be verified as current, accurate, and complete?

Employees have access to their records and can request an amendment, correction, or deletion of their records when the records are inaccurate, relevant, timely, or complete in accordance with the Privacy Act.

h. How will the information be collected (e.g. form, data transfer)?

Information will be collected from forms completed by the employee. Existing paper OPF records will be scanned into the e-OPF by OPM contractors. Data transfer also occurs via FPPS, WTTS and EEX.

2. INFORMATION NOT ABOUT INDIVIDUALS

a. Will information not about individuals be maintained in this system?

No

(1) If yes, identify the type of information (be specific).

b. What is the source of this information? Will it come from internal agency sources and/or external sources? Explain in detail.

C. USES OF SYSTEM AND INFORMATION

These questions will identify the use of the information and the accuracy of the data being used.

1. Describe all uses made of the data in this system:

- *Making a decision when an NRC employee or former NRC employee questions the validity of a specific document in an individual's record;*
- *Upon transfer of an employee to another Federal agency, the information is transferred to such agency;*
- *Store and query all personnel actions and related documentation;*
- *OPM investigations;*
- *Office of the Inspector General investigations;*
- *Security investigations;*
- *Determine eligibility for Federal benefits;*
- *Employment verification;*
- *Update monthly Enterprise Human Resources Integration data repository;*
- *Provide statistical reports to Congress, agencies, and the public on characteristics of the Federal work force;*
- *Review, audit, or reporting purposes by OPM and/or MSPB;*
- *Provide members of the public with the names, position titles, grades,*
- *Salaries, appointments (temporary or permanent), and duty stations of employees; and*
- *Provide information to the Public Health Service in connection with Health Maintenance Examinations and to other Federal agencies responsible for Federal benefit programs administered by the Department of Labor (Office of Workers= Compensation Programs) and the OPM.*

2. Is the use of the data both relevant and necessary for the purpose for which the system is designed?

Yes

3. Who will ensure the proper use of the data in this system?

HR Professionals and System Administrators

4. Are the data elements described in detail and documented?

Yes

a. If yes, what is the name of the document that contains this information and where is it located?

The data model can be found in the United States Office of Personnel Management Human Resources Line of Business Data Model Version 1: https://www.opm.gov/egov/documents/architecture/HRLOB_DM.pdf.

5. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

No

Derived data is obtained from a source for one purpose and then the original information is used to deduce/infer a separate and distinct bit of information that is aggregated to form information that is usually different from the source information.

Aggregation of data is the taking of various data elements and then turning it into a composite of all the data to form another type of data (i.e. tables or data arrays).

a. If yes, how will aggregated data be maintained, filed, and utilized?

b. How will aggregated data be validated for relevance and accuracy?

c. If data are consolidated, what *controls* protect it from unauthorized access, use, or modification?

6. How will data be *retrieved* from the system? Will data be retrieved by an individual's name or personal identifier? (Be specific.)

Records are retrieved by name and/or social security number.

7. Will this system provide the capability to identify, locate, and monitor (e.g., track, observe) individuals?

No

a. If yes, explain.

(1) What controls will be used to prevent unauthorized monitoring?

8. List the report(s) that will be produced from this system:

- *Active Documents- Created by HR Professionals*
- *Active Documents - Modifications*
- *Active Documents - Viewed*
- *Documents Moved to Deleted Folder*
- *Purged Documents- All Actions*
- *Purged Documents*
- *Inactive User*
- *New Employee*
- *eOPF Additional Access*
- *eOPF Roles*
- *eOPF User Information*

a. What are the reports used for?

Active Documents - ***Created by HR Professionals****: Allows the user to produce a report for either a specific individual's folder or to look at "create actions" performed by specific individuals that may span multiple folders. Using the "Filter by Viewer SSN," option you are looking for all actions performed by that individual.*

Active Documents - Modifications: *Allows the user to produce a report for either a specific individual's folder or to look at modification actions performed by a specific individual that may span multiple folders.*

Active Documents - Viewed: *Allows the user to produce a report for either a specific individual's folder or to look at "view actions" performed by a specific individual that may span multiple folders.*

Documents Moved to Deleted Folder: *Allows the user to produce a report for either a specific individual's folder or to look at "documents moved" actions performed by specific individuals that may span multiple folders.*

Purged Documents- All Actions: *Allows the user to produce a report for either a specific individual's folder "purged documents activities" or to look at all "purged documents activities" performed by specific individuals that may span multiple folders.*

Purged Documents*: Allows the user to produce a report for either a specific individual's folder for purged documents or to look at purge document action performed by a specific individuals that may span multiple folders.*

Inactive User: *Lists the employee accounts that have been inactivated by the employee feed provided to eOPF. The report displays the employee's current eOPF folder status. NOTE: The employee feed is*

configured to allow a time frame to occur between receipt of an employee 'Inactive' status and the time the employee account is disabled.

***New Employee**: Lists the eOPF accounts that have a folder and that have been created within a specified range of time. The following report uses the create date of the folder associated to the user account to determine if it falls within the specified date range.*

***eOPF Additional Access**: Displays the user's additional access rights in the eOPF system.*

***eOPF Roles:** Lists the user's Group membership(s) and Role in eOPF system.*

***eOPF User Information**: Lists the user account information.*

b. Who has access to these reports?

Access to reports is role based assigned by the HR System Administrator. The administrator can create a group to assign report access to; for example, access could be granted to all HR Professionals, or to just a special group of HR Professionals.

D. ACCESS TO DATA

1. Which NRC office(s) will have access to the data in the system?

Office of the Chief Human Capital Officer (OCHCO), regional HR staffs, and the Office of the Inspector General (OIG) have access to the data.

(1) For what purpose?

To maintain employee personnel records.

(2) Will access be limited?

Yes, access will be limited to NRC HR professionals.

2. Will other NRC systems share data with or have access to the data in the system?

No

(1) If yes, identify the system(s).

N/A

(2) How will the data be transmitted or disclosed?

N/A

3. Will external agencies/organizations/public have access to the data in the system?

Yes

(1) If yes, who?

OPM is the system owner and the data is hosted at OPM's data center.

(2) Will access be limited?

Yes, access will be limited through use of user logins and passwords or PIV/PIN, and role assignments.

(3) What data will be accessible and for what purpose/use?

OPM is authorized access to all Federal OPF records.

(4) How will the data be transmitted or disclosed?

Data can be transmitted from FPPS to the eOPF server using Connect: Direct or Connect: Direct Secure + Option.

E. RECORDS RETENTION AND DISPOSAL

The National Archives and Records Administration (NARA), in collaboration with federal agencies, approves whether records are temporary (eligible at some point for destruction/deletion because they no longer have business value) or permanent (eligible at some point to be transferred to the National Archives because of historical or evidential significance). These determinations are made through records retention schedules and are required under 36 CFR 1234.10. The following questions are intended to determine whether the records in the system have an approved records retention schedule or if one will be needed.

1. Can you map this system to an applicable retention schedule in NUREG-0910, or the General Records Schedules at http://www.archives.gov/records-mgmt/grs?

Yes

a. If yes, please cite the schedule number, approved disposition, and describe how this is accomplished. For example, will the records or a composite thereof be deleted once they reach their approved retention or exported to a file for transfer based on their approved disposition?

GRS 2.2 Item 040 Official Personnel Folder / electronic OPF (eOPF) (Long Term Records): Destroy 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.

GRS 2.2 Item 041 Official Personnel Folder / electronic OPF (eOPF) (Short Term Records): *Destroy when superseded or obsolete, or upon separation or transfer of employee, whichever is earlier.*

GRS 5.2 Item 020 Enterprise Human Resource Integration:
Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.

b. If the answer to question E.1 is yes, skip to F.1. If the response is no, complete question E.2 through question E.7.

2. If the records cannot be mapped to an approved records retention schedule, how long do you need the records? Please explain.

3. Would these records be of value to another organization or entity at some point in time? Please explain.

4. How are actions taken on the records? For example, is new data added or updated by replacing older data on a daily, weekly, or monthly basis?

5. What is the event or action that will serve as the trigger for updating, deleting, removing, or replacing information in the system? For example, does the information reside in the system for three years after it is created and then is it deleted?

6. Is any part of the record an output, such as a report, or other data placed in ADAMS or stored in any other location, such as a shared drive or MS SharePoint?

7. Does this system allow for the deletion or removal of records no longer needed and how will that be accomplished?

F. TECHNICAL ACCESS AND SECURITY

1. Describe the security controls used to limit access to the system (e.g., passwords).

Access is limited through the use of user logins and passwords or PIV card and PIN. Employees can only view their own information. HR System administrators implement and maintain user access for HR staff and investigators.

2. What controls will prevent the misuse (e.g., unauthorized browsing) of system data by those having access?

There are reports available for monitoring use of the system by each agency. Additional reports can be generated if needed.

3. Are the criteria, procedures, controls, and responsibilities regarding access to the system documented?

Yes

(1) If yes, where?

The eOPF Solution System Design Document available by request.

4. Will the system be accessed or operated at more than one location (site)?

No

a. If yes, how will consistent use be maintained at all sites?

5. Which user groups (e.g., system administrators, project managers, etc.) have access to the system?

Users of NRC records (HR Professionals, employees, supervisors) and system administrators (NRC, OPM).

6. Will a record of their access to the system be captured?

Yes

a. If yes, what will be collected?

All activities performed are tracked; for example, adding a document, deleting a document, creating an employee OPF. Any time an employee OPF is accessed, the system tracks each document that was viewed, and the reason why the document was viewed.

7. Will contractors be involved with the design, development, or maintenance of the system?

Yes

If yes, and if this system will maintain information about individuals, ensure Privacy Act and/or PII contract clauses are inserted in their contracts.

- *FAR clause 52.224-1 and FAR clause 52.224-2 should be referenced in all contracts, when the design, development, or operation of a system of records on individuals is required to accomplish an agency function.*
- *PII clause, "Contractor Responsibility for Protecting Personally Identifiable Information" (June 2009), in all contracts, purchase orders, and orders against other agency contracts and interagency agreements that involve contractor access to NRC owned or controlled PII.*

8. What auditing measures and technical safeguards are in place to prevent misuse of data?

There are reports available for monitoring use of the system by each agency. Additional reports can be generated if needed.

9. Are the data secured in accordance with FISMA requirements?

Yes

a. If yes, when was Certification and Accreditation last completed?

eOPF was authorized by OPM.

PRIVACY IMPACT ASSESSMENT REVIEW/APPROVAL
(For Use by OCIO/GEMS/ISB Staff)

System Name: Electronic Official Personnel Folder (eOPF)

Submitting Office: Office of Chief Human Capital Officer

A. PRIVACY ACT APPLICABILITY REVIEW

___ Privacy Act is not applicable.

__X__ Privacy Act is applicable.

Comments:
The e-OPF will not collect or maintain any PII on members of the public, only on current and former Federal employees. NRC OPF records are covered by NRC Privacy Act System of Records, NRC-11.

Reviewer's Name	Title	Date
Sally A. Hardy	Privacy Officer	5/11/2018

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION

__X__ No OMB clearance is needed.

___ OMB clearance is needed.

___ Currently has OMB Clearance. Clearance No._____

Comments:

Reviewer's Name	Title	Date
David Cullison	Agency Clearance Officer	4/24/18

C. RECORDS RETENTION AND DISPOSAL SCHEDULE DETERMINATION

___ No record schedule required.

____ Additional information is needed to complete assessment.

____ Needs to be scheduled.

_X_ Existing records retention and disposition schedule covers the system - no modifications needed.

Comments:

Reviewer's Name	Title	Date
Marna B. Dove	Sr. Program Analyst, Electronic Records Manager	5/10/18

D. BRANCH CHIEF REVIEW AND CONCURRENCE

_X_ This IT system **does not** collect, maintain, or disseminate information in identifiable form from or about members of the public.

____ This IT system **does** collect, maintain, or disseminate information in identifiable form from or about members of the public.

I concur in the Privacy Act, Information Collections, and Records Management reviews:

/RA/ Date May 15, 2018

Anna T. McGowan, Chief
Information Services Branch
Governance & Enterprise Management
Services Division
Office of the Chief Information Officer

TRANSMITTAL OF PRIVACY IMPACT ASSESSMENT/
PRIVACY IMPACT ASSESSMENT REVIEW RESULTS

TO: **Miriam Cohen, Chief Human Capital Officer, Office of Chief Human Capital Officer**	
Name of System: **Electronic Official Personnel Folder (eOPF)**	
Date ISB received PIA for review: **April 12, 2018**	Date ISB completed PIA review: **May 11, 2018**
Noted Issues: This system maintains records covered by NRC's Privacy Act system of records, NRC-11, General Personnel Records (Official Personnel Folder and Related Records). The e-OPF will not collect or maintain any PII on members of the public, only on current and former Federal employees.	
Anna T. McGowan, Chief Information Services Branch Governance & Enterprise Management Services Division Office of the Chief Information Officer	Signature/Date: **/RA/ May 15, 2018**
Copies of this PIA will be provided to: *Tom Rich, Director* *IT Services Development & Operation Division* *Office of the Chief Information Officer* *Jonathan Feibus* *Chief Information Security Officer (CISO)* *Governance & Enterprise Management Services Division* *Office of the Chief Information Officer*	