**Privacy Impact Assessment
Electronic Official Personnel Folder (eOPF)**

**Office of the Chief Information Officer (OCIO)/
Office of the Chief Human Capital Officer (OCHCO)**

**Version 3.0
04/16/2025**

Document Revision History

Date	Version	PIA Name/Description	Author
04/16/2025	3.0	eOPF - Transferred to the latest template, updated Points of Contact and Categories of Information	OCIO / OCHCO Oasis Systems, LLC
04/03/2025	DRAFT of 3.0	eOPF - DRAFT - Transferred to the latest template, updated Points of Contact	OCIO / OCHCO Oasis Systems, LLC
07/24/2024	2.0	eOPF - FINAL - Transferred to the latest template, updated Points of Contact	OCIO / OCHCO Oasis Systems, LLC
07/12/2024	DRAFT of 2.0	eOPF - DRAFT - Transferred to the latest template, updated Points of Contact	OCIO / OCHCO Oasis Systems, LLC
10/27/2023	1.0	eOPF - FINAL Release	OCIO / OCHCO Oasis Systems, LLC
10/03/2023	DRAFT	eOPF – DRAFT Release	OCIO / OCHCO Oasis Systems, LLC

Table of Contents

The agency is subject to the requirements of the E-Government Act and is committed to identifying and addressing privacy risks whenever it develops or makes changes to its information systems. The questions below help determine any privacy risks related to the E-Government Act or later guidance by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST).

Name/System/Subsystem/Service Name: Electronic Official Personnel Folder (eOPF).

Data Storage Location: (i.e., Database Server, SharePoint, Cloud, Other Government Agency, Power Platform): Other Federal Government Agency: U.S. Office of Personnel Management (OPM).

Date Submitted for review/approval: May 9, 2025.

1 Description

1.1 Provide the description of the system/subsystem, technology (i.e., Microsoft Products), program, or other data collections (hereinafter referred to as "project"). Explain the reason the project is being created.

The Electronic Official Personnel Folder (eOPF) system is owned by the U.S. Office of Personnel Management (OPM) Office of the Chief Information Officer Federal Data Solutions Data Warehouse Program. eOPF was developed by OPM for all Federal agencies as an e-Government initiative to manage and administer the official personnel files and to provide online access to personnel information for Human Resources (HR) staff, managers, and employees.

Each Federal employee has an Official Personnel Folder (OPF) which documents their entire period of Federal civilian service. The eOPF system maintains the electronic versions of the OPF for Federal employees and contains various official personnel files and human resource records used by the HR office. Each Federal employee has read only access to their individual folder in eOPF. The U.S. Nuclear Regulatory Commission (NRC) staff with assigned roles and responsibilities manage the NRC's users and data within the eOPF system.

Please mark appropriate response below if your project/system will involve the following:

☐ PowerApps	☐ Server/Database Design
☐ Dashboard	☐ Public Website
☐ SharePoint	☐ Internal Website
☐ Cloud Service Provider	☒ Other Web-based system owned and operated by OPM

1.2 Does this privacy impact assessment (PIA) support a proposed new project, proposed modification to an existing project, or other situation? Select options that best apply in table below.

Mark appropriate response.

Status Options	
☐	New system/project
☐	Modification to an existing system/project. *If modifying or making other updates to an existing system/project, provide the ADAMS ML of the existing PIA and describe the modification.*
☒	Annual Review *If making minor edits to an existing system/project, briefly describe the changes below.* Updated into the new template and updated Points of Contact.
☐	Other (explain)

1.3 Points of Contact:

Role	Contact Information Name Office/Division/Branch Phone Number
Project Manager(s)	Kevin Jones Office of the Chief Human Capital Officer (OCHCO)/Human Capital Analysis Branch (HCAB) 301-287-0573
System Owner/Data Owner or Steward	Jennifer Golder Office of the Chief Human Capital Officer (OCHCO) 301-287-0741
ISSM	Natalya Bobryakova Office of the Chief Information Officer (OCIO) /Cyber and Information Security Division (CISD) /Information Assurance and Oversight Branch (IAOB) 301-287-0671
Executive Sponsor	Jennifer Golder Office of the Chief Human Capital Officer (OCHCO) 301-287-0741

Role	Contact Information Name Office/Division/Branch Phone Number
Other	**Business Project Manager:** Karen Cobbs Office of the Chief Human Capital Officer (OCHCO) /Associate Director for HR Operations and Policy (ADHROP) / Workforce Management & Benefits Branch (WMBB) **Technical Project Manager:** Brendan Cain Office of the Chief Human Capital Officer (OCHCO) /Human Capital Analysis Branch (HCAB) 301-287-0552

2 Authorities and Other Requirements

2.1 What specific legal authorities and/or agreements permit the collection of information for the project?

Provide all statutory and regulatory authorities for operating the project, including the authority to collect the information; NRC internal policy is not a legal authority. Please mark appropriate response in table below.

Mark with an "X" on all that apply.	Authority	Citation/Reference
☒	**Statute**	*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 PIA Template (12-2020) 12 schedules and NARA statutes (44 United States Code (U.S.C.), 36 Code of Federation Regulations (CFR)). Under 36 CFR 1234.10, agencies are required to establish procedures for addressing records management requirements, including recordkeeping requirements and disposition, before approving new electronic information systems or enhancements to existing*

Mark with an "X" on all that apply.	Authority	Citation/Reference
		systems. The following question is intended to determine whether the records and data/information in the system have approved records retention schedule and disposition instructions, whether the system incorporates Records and Information Management and NARA's Universal Electronic Records Management requirements, and if a strategy is needed to ensure compliance.
☒	**Executive Order**	In general, OPM collects and maintains the information in eOPF pursuant to 5 United States Code (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.
☒	**Federal Regulation**	5 Code of Federation Regulations (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.
☐	**Memorandum of Understanding/Agreement**	
☐	**Other (summarize and provide a copy of relevant portion)**	

2.2 Explain how the information will be used under the authority listed above (*i.e., enroll employees in a subsidies program to provide subsidy payment*)**.**

The data is used by HR personnel for human resource functions. Each NRC employee can view their personnel forms and information in eOPF.

If the project collects Social Security numbers, state why this is necessary and how it will be used.

Information in eOPF is indexed/filed using the Social Security Number (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. Records can be retrieved by employee name and/or SSN.

3 Characterization of the Information

In the table below, mark the categories of individuals for whom information is collected.

Category of individual	
☒	Federal employees
☐	Contractors
☐	Members of the Public (any individual other than a federal employee, consultant, or contractor)
☐	Licensees
☒	Other: Former NRC employees

In the table below, is a list of the most common types of PII collected. Mark all PII that is collected and stored by the project/system. If there is additional PII not defined in the table below, a comprehensive listing of PII is provided for further reference in ADAMS at the following link: PII Reference Table.

Categories of Information			
☒	Name	☒	Resume or curriculum vitae
☒	Date of Birth	☐	Driver's License Number
☐	Country of Birth	☐	License Plate Number
☐	Citizenship	☐	Passport number
☐	Nationality	☒	Relatives Information
☐	Race	☐	Taxpayer Identification Number
☒	Home Address	☐	Credit/Debit Card Number
☒	Social Security number (Truncated or Partial)	☒	Medical/health information
☐	Sex (Male or Female)	☐	Alien Registration Number
☐	Ethnicity	☒	Professional/personal references

Categories of Information			
☒	Spouse Information	☒	Criminal History
☐	Personal e-mail address	☐	Biometric identifiers (facial images, fingerprints, iris scans)
☒	Personal Bank Account Number	☒	Emergency contact e.g., a third party to contact in case of an emergency
☒	Personal Mobile Number/Home Number	☒	Accommodation/disabilities information
☐	Marital Status	☒	Other: eOPF may contain military service information, health and/or life insurance policy numbers, Thrift Savings Plan election and changes, veteran's preference designation and verification, 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.
☒	Children Information		
☐	Mother's Maiden Name		

3.1 Describe how the data is collected for the project. (i.e., NRC Form, survey, questionnaire, existing NRC files/ databases, response to a background check).

The NRC HR specialists submit forms to eOPF for filing in an employee's eOPF. The information on the forms is completed by the individual or by the HR specialists.

3.2 If using a form (paper or web) to collect the information, provide the form number, title and/or a link to the form.

N/A.

3.3 Who provides the information? Is it provided directly from the individual or a third party.

The information maintained in eOPF is provided by the individual and agency's HR specialists.

3.4 Explain how the accuracy of the data collection is validated. If the project does not check for accuracy, please explain why.

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

3.5 Will PII data be used in a test environment? If so, explain the rationale for this and how the PII information is protected.

No.

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

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

4 Data Security

4.1 Describe who has access to the data in the project (i.e., internal NRC, system administrators, external agencies, contractors, public).

NRC's Office of the Chief Human Capital Officer (OCHCO), the Office of the Inspector General (OIG), and employees have access to the data.

4.2 If the project/system shares information with any other NRC systems, identify the system, what information is being shared and the method of sharing.

N/A.

4.3 If the project/system connects, receives, or shares information with any external non-NRC partners or systems, identify what is being shared.

The information in eOPF may be shared for background investigation purposes with Defense Counterintelligence and Security Agency (DCSA) investigators, who access OPF to perform work during investigations such as initial background checks and renewal of existing investigations.

If so, identify what agreements are in place with the external non-NRC partner or system in the table below.

	Agreement Type
☐	Contract 　　　Provide Contract Number:
☐	License 　　　Provide License Information:
☐	Memorandum of Understanding 　　　Provide ADAMS ML number for MOU:
☒	Other: DCSA is not authorized to conduct a background investigation unless a release, signed by the subject of the investigation is received.
☐	None

4.4 Describe how the data is accessed and describe the access control mechanisms that prevent misuse.

eOPF employs role-based access controls, which categorize users as employee, Investigator, HR Specialist, or agency administrator, and permits access according to user's role. Authorized users can authenticate to eOPF using a Personal Identity Verification (PIV) card credentials or Login.gov account.

4.5 Explain how the data is transmitted and how confidentiality is protected (i.e., encrypting the communication or by encrypting the information before it is transmitted).

Data can be transmitted through a secure web connection (HTTPS) from FPPS to the eOPF server using Connect: Direct or Connect: Direct Secure + Option.

4.6 Describe where the data is being stored (i.e., NRC, Cloud, Contractor Site).

eOPF is hosted by the Office of Personnel Management (OPM) in the Macon Data Center.

4.7 Explain if the project can be accessed or operated at more than one location.

No.

4.8 Can the project be accessed by a contractor? Have the contractors completed an IT-II investigation? Do they possess an NRC badge?

Yes, eOPF can be accessed by a contractor. Any OCHCO contractors that might access eOPF are badged.

This system will maintain information about individuals, ensure Privacy Act and/or Personally Identifiable Information (PII) contract clauses are inserted in their contracts.

- *Federal Acquisition Regulation (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.*

4.9 Explain the auditing measures and technical safeguards 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.

4.10 Describe if the project has the capability to identify, locate, and monitor (i.e., trace/track/observe) individuals.

No.

4.11 Define which FISMA boundary this project is part of.

NRC's eOPF is a component of Third-Party System (TPS) OCHCO External Services (OES) Subsystem.

4.12 Is there an Authority to Operate (ATO) associated with this project/system?

The OPM issued an Authority to Operate (ATO) for eOPF on July 8, 2019.

NRC issued an ongoing ATO for the TPS-OES subsystem on December 20, 2018, (ADAMS accession number ML18354A944).

Authorization Status	
☐	Unknown
☐	No *If no, please note that the authorization status must be reported to the Chief Information Security Officer (CISO) and Computer Security Organization (CSO's) Point of Contact (POC) via e-mail quarterly to ensure the authorization remains on track.*
☐	In Progress provide the estimated date to receive an ATO. Estimated date:
☒	Yes Indicate the data impact levels (Low, Moderate, High, Undefined) approved by the Chief Information Security Officer (CISO) Confidentiality-Moderate Integrity-Moderate Availability-Moderate

4.13 Provide the NRC system Enterprise Architecture (EA)/Inventory number. If unknown, contact EA Service Desk to get the EA/Inventory number.

The TPS EA number is 20180002.

Guidance for retentions comes from the Office of Personnel Management's *The Guide to Personnel Recordkeeping*, OPM/GOVT-1 SORN and NARA's GRS 2.2 – Employee Management Records and GRS 5.2 – Transitory and Intermediary Records.

5   Privacy Act Determination

5.1 Is the data collected retrieved by a personal identifier?

Mark the appropriate response.

	Response
☒	**Yes, the PII is retrieved by a personal identifier (i.e., individual's name, address, SSN, or other unique number, etc.)** **List the identifiers that will be used to retrieve the information on the individual.** Name, SSN, Address, Date of Birth, and Medical/health information.
☐	**No, the PII is not retrieved by a personal identifier.** **If no, explain how the data is retrieved from the project.**

5.2 For all collections where the information is retrieved by a personal identifier, the Privacy Act requires that the agency publish a System of Record Notice (SORN) in the Federal Register. *As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some other personal identifier assigned to the individual.*

Mark the appropriate response in the table below.

	Response
☒	***Yes, this system is covered by an existing SORN. (See existing SORNs: https://www.nrc.gov/reading-rm/foia/privacy-systems.html)*** ***Provide the SORN name, number, (List all SORNs that apply):*** Government-wide SORN: OPM/GOVT-1 – General Personnel Records
☐	**SORN is in progress**
☐	**SORN needs to be created**
☐	**Unaware of an existing SORN**
☐	**No, this system is not a system of records and a SORN is not applicable.**

5.3 When an individual is asked to provide personal data (i.e., form, webpage, survey), is a Privacy Act Statement (PAS) provided?

A Privacy Act Statement is a disclosure statement required to appear on documents used by agencies when an individual is asked to provide personal data. It is required for any forms, surveys, or other documents, including electronic forms, used to solicit personal information from individuals that will be maintained in a system of records.

Mark the appropriate response.

Options	
☒	**Privacy Act Statement**
☐	**Not Applicable**
☐	**Unknown**

5.4 Is providing the PII mandatory or voluntary? What is the effect on the individual by not providing the information?

Providing PII is mandatory.

6 Records and Information Management-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). Records/data and information with historical value, identified as having a "permanent" disposition, are transferred to the National Archives of the United States at the end of their retention period. All other records identified as having a "temporary" disposition are destroyed at the end of their retention period in accordance with the NARA Records Schedule or the General Records Schedule.

These determinations are made through records retention schedules and NARA statutes (44 United States Code (U.S.C.), 36 Code of Federation Regulations (CFR)). Under 36 CFR, agencies are required to establish procedures for addressing Records and Information Management (RIM) requirements. This includes strategies for establishing and managing recordkeeping requirements and disposition instructions before approving new electronic information systems or enhancements to existing systems.

The following questions are intended to determine whether the records/data and information in the system have approved records retention schedules and disposition instructions, whether the system incorporates RIM strategies including support for NARA's Universal Electronic Records Management (ERM) requirements, and if a mitigation strategy is needed to ensure compliance.

If the project/system:

- Does not have an approved records retention schedule and/or
- Does not have an *automated* RIM functionality,
- Involves a cloud solution,
- And/or if there are additional questions regarding Records and Information Management - Retention and Disposal, please contact the NRC Records staff at **ITIMPolicy.Resource@nrc.gov** for further guidance.

If the project/system has a record retention schedule or an automated RIM functionality, please complete the questions below.

6.1 Does this project map to an applicable retention schedule in NRC's Comprehensive Records Disposition Schedule (NUREG-0910), or NARA's General Records Schedules?

☐	NUREG-0910, "NRC Comprehensive Records Disposition Schedule
☒	NARA's General Records Schedules
☐	Unscheduled

6.2 If so, cite the schedule number, approved disposition, and describe how this is accomplished.

System Name (include sub-systems, platforms, or other locations where the same data resides)	eOPF
Records Retention Schedule Number(s)	GRS 2.2 Item 040 Official Personnel Folder (Long Term Records) GRS 2.2 Item 041 Official Personnel Folder (Short Term Records) GRS 5.2 Item 020 Enterprise Human Resource Integration
Approved Disposition Instructions	GRS 2.2 Item 040 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 Destroy when superseded or obsolete, or upon separation or transfer of employee, whichever is earlier GRS 5.2 Item 020 Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever

	is later. (Hardcopy original personnel folders scanned into the Enterprise Human Resource Integration (EHRI) eOPF Database are covered by this item)
	See Chapter 7 of The Guide to Personnel Recordkeeping for guidance for processing personnel records for:
	Transferring eOPF
	• Serviced by a different personnel office in the same agency; • In another agency when both offices transfer personnel and medical folders; and • In an agency that does not transfer personnel and medical folders.
	Transferring Records to the National Personnel Records Center (NPRC)
	Under normal circumstances, the eOPF is transferred to NPRC 90 days after separation from Federal service.
Is there a current automated functionality or a manual process to support RIM requirements? This includes the ability to apply records retention and disposition policies in the system(s) to support records accessibility, reliability, integrity, and disposition.	Electronic Official Personnel Folder (eOPF) system is owned by the U.S. Office of Personnel Management (OPM) Office of the Chief Information Officer Federal Data Solutions Data Warehouse Program and is responsible for the retention of its data.
Disposition of Temporary Records Will the records/data or a composite be automatically or manually deleted once they reach their approved retention?	Yes

Disposition of Permanent Records Will the records be exported to an approved format and transferred to the National Archives based on approved retention and disposition instructions? If so, what formats will be used? **NRC Transfer Guidance (Information and Records Management Guideline - IRMG)**	N/A

7   Paperwork Reduction Act

The Paperwork Reduction Act (PRA) of 1995 requires that agencies obtain an Office of Management and Budget (OMB) approval in the form of a "control number"—before promulgating a paper form, website, surveys, questionnaires, or electronic submission from 10 or more members of the public. If the data collection is from federal employees regarding work-related duties, then a PRA clearance is not necessary.

7.1 Will the project be collecting any information from 10 or more persons who are not Federal employees?

No.

7.2 Is there any collection of information addressed to all or a substantial majority of an industry (i.e., Fuel Fabrication Facilities or Fuel Cycle Facilities)?

No.

7.3 Is the collection of information required by a rule of general applicability?

No.

Note: For information collection (OMB clearances) questions: contact the NRC's Clearance Officer. Additional guidance can be found on the NRC's internal Information Collections Web page at: https://intranet.nrc.gov/ocio/33456.

8 Privacy Act Determination

Project/System Name: Electronic Official Personnel Folder (eOPF)

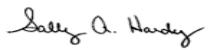**Submitting Office:** Office of the Chief Human Capital Officer (OCHCO)

Privacy Officer Review

	Review Results	Action Items
☐	This project/system **does not contain PII.**	**No further action** is necessary for Privacy.
☐	This project/system **does contain PII**; the Privacy Act does **NOT** apply, since information is NOT retrieved by a personal identifier.	**Must be protected with restricted access** to those with a valid need-to-know.
☒	This project/system **does contain PII**; the **Privacy Act does apply**.	**SORN is required-** Information is **retrieved** by a personal identifier**.**

Comments:

Covered by Government-wide SORN: OPM/GOVT-1 – General Personnel Records.

Reviewer's Name	Title
Sally A. Hardy Signed by Hardy, Sally on 05/23/25	Privacy Officer

9   OMB Clearance Determination

NRC Clearance Officer Review

	Review Results
☒	No OMB clearance is needed.
☐	OMB clearance is needed.
☐	Currently has OMB Clearance. Clearance No._____

Comments:

Reviewer's Name	Title
Karen C Benney Signed by Benney, Kristen on 04/24/25	Agency Clearance Officer
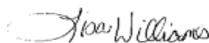
10 Records Retention and Disposal Schedule Determination

Records Information Management Review

Review Results	
☐	No record schedule required.
☐	Additional information is needed to complete assessment.
☐	Needs to be scheduled.
☒	Existing records retention and disposition schedule covers the system - no modifications needed.

Comments:

Reviewer's Name	Title
Signed by Dove, Marna on 05/22/25	Sr. Program Analyst, Electronic Records Manager
Signed by Williams, Lisa on 05/06/25	Records and Information Management Specialist

11 Review and Concurrence

	Review Results
☐	This project/system **does not** collect, maintain, or disseminate information in identifiable form.
☒	This project/system **does** collect, maintain, or disseminate information in identifiable form.

I concur with the Privacy Act, Information Collections, and Records Management reviews.

Signed by Nalabandian, Garo
    on 05/29/25

Director
Chief Information Security Officer
Cyber Information Security Division
Office of the Chief Information Officer

ADDITIONAL ACTION ITEMS/CONCERNS

Name of Project/System: Electronic Official Personnel Folder (eOPF)	
Date CISD received PIA for review: April 22, 2025	**Date CISD completed PIA review:** May 23, 2025
Action Items/Concerns:	