U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: Federal Human Resources Navigator (FedHR Navigator)
Bureau/Office: Office of the Secretary
Date: September 28, 2018
Point of Contact
Name: Teri Barnett
Title: Departmental Privacy Officer
Email: DOI_Pivacy@ios.doi.gov
Phone: (202) 208-1605
Address: 1849 C Street NW, Room 7112, Washington, DC 20240

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on
- ☐ Members of the general public
- ☒ Federal personnel and/or Federal contractors
- ☐ Volunteers
- ☐ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

The Federal Human Resources (FedHR) Navigator is an enterprise Human Resources (HR) system that contains web-based software tools that support human capital strategic management within the Department of the Interior (DOI). The DOI Office of Human Resources contracted with Economic Systems (EconSys) to develop the FHR Navigator for Department-wide use. The

FHR navigator tools are located in a secured, centralized database that is accessible by authorized DOI employees, including HR personnel. The main tool within the application is the Federal Retirement Benefits (FRB) Web, which is a calculator that generates Federal employee retirement benefits information.

The purpose of this system is to electronically calculate and track employee retirement annuity benefits, calculate service computation date, and provide benefits counseling. Annuity is based on pay and other factors that impact and employee's retirement annuity. The analysis report from FedHR Navigator pre-populates information that helps HR benefits personnel determine annuity benefits and produce FRB reports. HR Benefits Specialists can view a Federal employee's record in the FedHR Navigator system to assist employees inquiring about their retirement. FedHR Navigator is used by DOI bureaus and offices including the Bureau of Indian Affairs (BIA), Bureau of Land Management (BLM), Bureau of Reclamation (BOR), and the U.S. Fish and Wildlife Service (FWS). Each bureau has their own instance and implementation of FedHR Navigator and is responsible for complying with Federal and Departmental legal and policy requirements.

C. What is the legal authority?

5 U.S.C. 5101, et seq., Government Organization and Employees; 31 U.S.C. 3512, et seq., Executive Agency Accounting and Other Financial Management Reports and Plans; 31 U.S.C. 1101, et seq., the Budget and Fiscal, Budget, and Program Information; 5 CFR part 293, subpart B, Personnel Records Subject to the Privacy Act; 5 CFR part 297, Privacy Procedures for Personnel Records; Executive Order 9397 as amended by Executive Order 13478, relating to Federal agency use of Social Security numbers; and Public Law 101–576 (Nov. 15, 1990), Chief Financial Officers (CFO) Act of 1990.

D. Why is this PIA being completed or modified?

☐ New Information System
☐ New Electronic Collection
☒ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other: *Describe*

E. Is this information system registered in CSAM?

☒ Yes: *Enter the UII Code and the System Security Plan (SSP) Name*

UII Code: 010-999991241, FedRAMP System Security Plan (SSP)

☐ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	Purpose	Contains PII *(Yes/No)*	Describe *If Yes, provide a description.*
None	None	No	N/A

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☒ Yes: *List Privacy Act SORN Identifier(s)*

Records in FedHR Navigator are maintained under maintained under INTERIOR/DOI-85, Payroll, Attendance, Retirement, and Leave Records, 83 FR 34156, July 19, 2018; and OPM/GOVT-1, General Personnel Records, 71 FR 35342, December 11, 2012.

☐ No

H. Does this information system or electronic collection require an OMB Control Number?

☐ Yes: *Describe*
☒ No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

☒ Name
☒ Birth Date
☒ Medical Information
☒ Social Security Number (SSN)
☒ Employment Information
☒ Military Status/Service
☒ Mailing/Home Address
☒ Other: *Specify the PII collected.*

Employee data is imported from the Federal Personnel and Payroll System (FPPS), such as Social Security number (SSN), date of birth (DOB), home address, health/life insurance, leave, taxes, salary, military status/service information and service computation date. This information is required to calculate estimated Federal retirement benefits and provide retirement benefits counseling.

B. What is the source for the PII collected? Indicate all that apply.

☒ Individual
☐ Federal agency
☐ Tribal agency
☐ Local agency
☒ DOI records
☐ Third party source
☐ State agency
☐ Other: *Describe*

C. How will the information be collected? Indicate all that apply.

☒ Paper Format
☒ Email
☒ Face-to-Face Contact
☒Web site
☒ Fax
☒ Telephone Interview
☒ Information Shared Between Systems *Describe*

FPPS data is manually uploaded in batches into the FedHR Navigator system to calculate employee retirement benefits.

☐ Other: *Describe*

D. What is the intended use of the PII collected?

The system contains sensitive PII including SSN, salary information, and DOB, which is used to identify employees, calculate estimated Federal retirement benefits and provide retirement benefits counseling. The system is a tool that helps employees with financial/retirement planning and calculates retirement estimates based on specific employee data. HR staff use pay and leave data to offer benefits administration services, retirement counseling, and retirement package preparation. Specifically, salary history data and pay data is used to estimate annuity payments.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

Data is shared within the Office of Human Resources to calculate and track employee retirement annuity benefits, calculate service computation date, and provide benefits counseling.

☒ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

The data will be used within each bureau or office Servicing Personnel Office (SPO) to provide retirement and benefits services to employees. Within the SPO only certain HR Benefits Specialists use the data to estimate annuity payments for employees and provide benefits counseling. Data is not shared with other bureaus/offices as each bureau/office maintains and manages their own instance of the application.

☒ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

The employee retirement benefits package is sent to the Office of Personnel Management (OPM) for final processing. The information on the forms sent to OPM is used to qualify a retiree for health insurance, life insurance, and their retirement annuity. Information may be shared with other Federal agencies as permitted by the Privacy Act or as a routine use outlined in the published OPM/GOVT-1 and DOI-85 system of records notices.

☐ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

☒ Contractor: *Describe the contractor and how the data will be used.*

EconSys contractors provide operational and maintenance support for the system; however, they do not have access to PII.

☐ Other Third Party Sources: *Describe the third party source and how the data will be used.*

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

Each DOI bureau or office utilizes different methods for collecting information and providing the retirement benefits counseling.

BIA, BOR, and BLM employees voluntarily contact their SPO to request retirement benefits information from an HR Benefits Specialist. These employees must provide their PII in order to locate their record and accurately calculate annuity payments. Data is imported from FPPS into the FedHR Navigator system upon request of the employee for the service. If an employee does not request the service, the SPO will not import data or provide benefits counseling services.

FWS employees who request retirement benefits calculation are sent a request form by the SPO. This form includes their Name, SSN, DOB, and Length of Service. Employees are required to e-mail, fax or post mail the form back to the HR Benefits Specialist. The completed and returned form provides the employee's consent for the SPO to retrieve their PII from FPPS. If the request

form is not returned to the SPO, the SPO will not import data or provide benefits counseling services.

☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ Privacy Act Statement: *Describe each applicable format.*

A Privacy Act Statement is provided to individuals and is placed on bureau/office forms.

☒ Privacy Notice: *Describe each applicable format.*

Privacy notice is provided through the publication of this privacy impact assessment, the Privacy Act Statement provided on bureau/office forms, and the published systems of records notices DOI-85: Payroll, Attendance, Retirement and Leave Records and OPM/GOVT-1, General Personnel Records, which may be viewed at https://www.doi.gov/privacy/sorn.

☐ Other: *Describe each applicable format.*

☐ None

H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

Data is retrieved manually from FFPS and via reports using employee name or SSN. SSN is required to obtain employee pay information from FPPS for annuity calculations.

I. Will reports be produced on individuals?

☒ Yes: *What will be the use of these reports? Who will have access to them?*

Benefits reports are generated by the HR Benefits Specialist for individual employees. These reports are shared with the employee seeking retirement calculations or counseling. Audit logs are used to monitor user behavior and to prevent unauthorized access or actions.

☐ No

Section 3. Attributes of System Data

A. How will data collected from sources other than DOI records be verified for accuracy?

Information collected from FPPS is verified for accuracy through internal processes and is considered to be an accurate and current source of data on Federal employees for purposes of benefits counseling. Verification of data occurs in FPPS which contains validity and relational edits designed to ensure the data entry technician inputs accurate information. FPPS data fields have the capability to ensure that the data entered is correct and cannot be altered such as validating employee SSN; restricting the deletion of addresses; and requiring the use of numeric dates.

B. How will data be checked for completeness?

FPPS has data quality procedures in place to ensure the completeness and accuracy of employment data for pay and benefits. Data is checked for completeness by the FPPS prior to being extracted by FedHR Navigator. FedHR Navigator has secondary checks on validity prior to loading the FPPS data into the FedHR Navigator databases. All data is initially loaded into staging tables where validity checks are made, which includes verification that numbers are entered in number fields and dates are entered in date fields etc.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

The DOI records loaded into FedHR Navigator are manually extracted from the FPPS. The FPPS is refreshed each pay period or every two weeks and FPPS is considered to be an accurate and current source of data on Federal employees.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

As supporting information for HR processes, data in FHR Navigator is subject to the Department Records Schedule (DRS) 1.2.0004 - Short-Term Human Resources Records (DAA-0048-2013-0001-0004), which is approved by the National Archives and Records Administration (NARA). Benefits records have a temporary disposition. Records are cut off at the end of the fiscal year, and destroyed 3 years after cutoff. Records may also be maintained under other long-term records schedule, such as DRS 1.2C, Retirement and Payroll Records Warranting Extended Preservation (DAA-0048-2013-0001-0008), which is approved by NARA. The system generally maintains temporary records, and retention periods vary based on the type of record under each item and the needs of the agency.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

When approved for destruction, paper records are disposed of by shredding or pulping, and records contained on electronic media are degaussed or erased in accordance with NARA Guidelines and 384 Departmental Manual 1.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

There is a moderate risk to individual privacy due to the sensitive nature and volume of PII within the system that traverses the DOI computer network. FedHR Navigator has undergone a formal Assessment and Authorization for issuance of an authority to operate in accordance with the Federal Information Security Modernization Act (FISMA) and National Institute of Standards and Technology (NIST) guidelines. FedHR Navigator has been rated as a moderate system requiring strict security and privacy controls to protect the confidentiality, integrity, and availability of data in the system. As part of the continuous monitoring program, continuous auditing will occur on the system to identify and respond to potential impacts to the PII collected and used within the system.

There is a risk that information may be used outside the scope of the purpose for which it was collected or that internal employees may inappropriately handle PII that they have access to. This risk is mitigated by the HR Benefits Specialists complying with the DOI-wide privacy and security policies to reduce the possibility of such incidents and bureaus have internal controls in place to reduce PII loss. A Privacy Act Statement is displayed during initial access into the system to help mitigate possible PII loss. There are fines, penalties and disciplinary actions for breaches of PII so this assists in mitigating such unfavorable activities.

There is a risk that PII may be accessed by unauthorized personnel, such as in cases where an individual inappropriately accesses the system or an employee prints to a shared printer and fails to pick up the printed document. This risk is mitigated by the continuous monitoring activities and privacy and security practices that are implemented at DOI. This risk is mitigated by the access controls implemented to ensure only authorized personnel have access to the records needed to perform official duties. Access is based on *"need-to-know"* basis. Access to PII is limited to HR specialists or authorized personnel. FedHR users must sign the DOI Rules of Behavior which identifies the need to protect PII data prior to gaining access. Users must also complete annual security and privacy awareness training, as well as role-based training. User activity is monitored, and account access and denial, as well as any record changes are logged. These audit logs are reviewed by the system administrators for inappropriate use of the system and data.

There is a risk that data may not be appropriate to store in a cloud service provider's system, or that the vendor may not handle or store information appropriately according to DOI policy. FedHR Navigator is provided and hosted by a FedRAMP certified service provider and has met all requirements for information categorized as Moderate in accordance with FISMA. The

system requires strict security and privacy controls to protect the confidentiality, integrity, and availability of data in the system at the moderate level. The use of DOI Information Systems is conducted in accordance with the appropriate DOI Security and Privacy Control Standards policy and NIST guidelines. The cloud service provider is subject to all the Federal legal and policy requirements for safeguarding Federal information, and is responsible for preventing unauthorized access to the system and protecting the data contained within the system.

There is a risk that individuals may not have notice of the purposes for collecting their information, how it will be used, or that their PII is sourced from other DOI internal systems such as FPPS and shared internally with DOI officials or with OPM. Individuals are notified of the privacy practices through published DOI-85 and OPM/GOVT-1 systems of records notices, the Privacy Act Statement placed on form, and this PIA that provides a detailed description of system sources, data elements and how PII information is shared to help employees understand the system.

There is a risk that the system may collect, store or share more information than necessary, or the system will be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule. To mitigate this risk, access to data is restricted and authorized personnel only retrieve records on individuals upon the Federal employee's request for retirement benefits services. The data collected and stored is limited to the minimal amount of data needed to meet Federal retirement benefits calculations or counseling. Records are maintained and disposed of in accordance with records retention schedules that were approved by NARA. Users also are reminded through policy and training that they must follow the applicable retention schedules and requirements of the Federal Records Act.

Section 4. PIA Risk Review

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

☒ Yes: *Explanation*

The FedHR Navigator data is both relevant and necessary to provide benefits counseling services to Federal employees.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

C. Will the new data be placed in the individual's record?

☐ Yes: *Explanation*
☒ No

D. Can the system make determinations about individuals that would not be possible without the new data?

☐ Yes: *Explanation*
☒ No

E. How will the new data be verified for relevance and accuracy?

FedHR does not derive new data or create previously unavailable data about an individual through aggregation.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☒ Users
☒ Contractors
☐ Developers
☒ System Administrator
☒ Other: *Describe*

Only the HR Benefits Specialists working in the bureau/office SPO offices have access to data in the FedHR system. HR benefits specialists can view an employee's record in the FedHR Navigator system to assist employees inquiring about their retirement.

H. How is user access to data determined? Will users have access to all data or will access be restricted?

Access is restricted to HR Benefits Specialists that provide benefits counseling services. Authorized HR Benefits Specialists have access to all employee data in the system since they

may need to provide benefits counseling to an employee. Data is not shared between the bureaus and offices as they each have instances of the FedHR Navigator application.

EconSys creates starter accounts for the DOI HR administrators. After the account planning phase, EconSys creates the roles and permissions that DOI HR administrators will have available for their own user account management, user roles, use case permissions, and how DOI employees will be categorized for access by HR users.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

The FedHR Navigator software was designed and developed by EconSys, Inc. The software is provided as a service to DOI bureaus and offices. EconSys operates and maintains the system. Privacy Act clauses are included in their contracts.

☐ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐ Yes. *Explanation*
☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?

☐ Yes. *Explanation*
☒ No

L. What kinds of information are collected as a function of the monitoring of individuals?

FedHR Navigator is not designed to monitor individuals, except for monitoring user behaviors for security purposes. FedHR administrators use audit logs to prevent unauthorized use and user behaviors. Through this auditing process, usernames, IP addresses, time/date and login status are collected to support incident response and troubleshooting.

M. What controls will be used to prevent unauthorized monitoring?

Only administrators and account managers have access to information contained in the audit logs. These audit logs are used to ensure that accounts are valid, accurate and being used for the intended purpose. System privacy and security controls are also implemented and enforced to protect the system and information within the system.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☒ Security Guards
☐ Key Guards
☒ Locked File Cabinets
☒ Secured Facility
☒ Closed Circuit Television
☐ Cipher Locks
☒ Identification Badges
☐ Safes
☐ Combination Locks
☒ Locked Offices
☒ Other. *Describe*

FedHR Navigator is provided by and hosted by a FedRAMP certified service provider who has met all requirements for physical controls for information categorized as Moderate.

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☐ Biometrics
☒ Intrusion Detection System (IDS)
☒ Virtual Private Network (VPN)
☐ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☒ Other. *Describe*

In addition to DOI controls listed above, FedHR Navigator is provided by and hosted by a FedRAMP certified service provider who has met all requirements for technical controls for information categorized as Moderate.

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits
☒ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☒ Regular Monitoring of Users' Security Practices
☒ Methods to Ensure Only Authorized Personnel Have Access to PII
☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Privacy and Records Management Training

☐ Other. *Describe*

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The Director of Office of Human Resources serves as the FedHR Information System Owner and the official responsible for oversight and management of the FedHR security and privacy controls and the protection of the information processed and stored by the FedHR program area. The FedHR Information System Owner and the Information System Security Officer are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored within all FedHR program areas, and addressing Privacy Act requests and complaints in consultation with DOI Privacy Officials. Each DOI bureau or office is responsible for the management of their own data, protecting the privacy rights of the employees for the information they collect, maintain, and use in the system, and for meeting the requirements of the Privacy Act including any request for notification, access or amendment in consultation with privacy officials.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The FedHR System Owner and the Information System Security Officer are responsible for the daily operational oversight and management of the FedHR program security and privacy controls, and for ensuring to the greatest possible extent that data is properly managed and that access to the data has been granted in a secure and auditable manner. The FedHR Information System Owner, Information System Security Officer, and the program officials authorized to access the system are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC, and appropriate DOI officials in accordance with Federal policy and established DOI procedures. Each DOI bureau or office is responsible for the management of their own data, protecting the privacy rights of the employees for the information they collect, maintain, and use in the system, and for meeting the requirements of the Privacy Act, and reporting any potential loss, compromise, unauthorized access or disclosure of data resulting from their activities or management of the data.