

**Pension Benefit Guaranty Corporation (PBGC)
Privacy Impact Assessment (PIA)**



**Office of Management and Administration
Federal Risk and Authorization Management
Program
(OMAFedRAMP)**

Federal Human Resources (FedHR) Navigator

March 2023

1 Privacy Point of Contact

Name	Johane Pace
Title	Information System Owner
Phone	202-394-9224
Email	Pace.Johane@pbgc.gov

TIP!
This point of contact should be the person you want the Privacy Office to work with in completing this PIA. For some systems it might be the Information Owner (IO) or Information System Owner (ISO). Many business units identify this as the Information System Security Officer (ISSO). DO what makes sense for you!

2 Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is an analysis of how information is/will be handled:

- i. To ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy,
- ii. To determine risks and effects of collecting, maintaining, and disseminating information in an identifiable form in an electronic information system, and
- iii. To examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Privacy concerns are highest for systems that contain Personally Identifiable Information (PII). PII is defined as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Because there are many types of information that can be used to

TIP
Information that either alone or when considered with other information that uniquely identifies a person is Personally Identifiable Information (PII). Combining pieces of information whether private or publicly available has powerful implications for uniquely identifying an individual.

distinguish or trace an individual's identity, the term PII is necessarily broad.

For example, consider a person named Mary Jones. There are over 200 million results in an internet search for this name. But if we combine information such as a date of birth, the last four digits of a (or worse, an entire) Social Security Number, or a spouse's name, the number of persons to whom we could be referring begins to narrow quite rapidly. These types of information are considered identifiers. Identifiers that uniquely identify a person are the focus of privacy protection.

2.1 The Components of the System

Name of component	Describe the component (1 or 2 sentences)	Does this component contain PII?	In what system of records (SORN) is this information stored?	What is the Legal Authority for collection of this information?	Does this system share PII externally? (please detail in question 9)
The Electronic Performance Management (e-Performance)	The e-Performance module is a web-based system that allows managers to create and approve Performance Appraisals and Performance Improvement Plans. Supervisors can route documents for approval and request that other users provide input for an employee's performance review; users can upload supporting documents as requested.	Yes	OPM/GOVT-2 -- Employee Performance File System Records OPM/GOVT-3 -- Records of Adverse Actions, Performance Based Reductions in Grade and Removal Actions, and Termination of Probationers	5 U.S.C. 1104, 3321, 4305, and 5405, and Executive Order 12107. 5 U.S.C. 3321 , 4303, 7504, 7514, and 7543.	Yes
Retirement/Benefit	The Retirement module an employee retirement package preparation, that allows employees and HR Specialists (Benefits) to engage simultaneously for retirement	Yes	OPM/GOVT-1 -- General Personnel Records OPM/GOVT-10 Employee Medical	5 U.S.C. 1302 , 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, 9830, and 12107. Executive Orders 12107, 12196, and 12564 and 5 U.S.C.	No

Name of component	Describe the component (1 or 2 sentences)	Does this component contain PII?	In what system of records (SORN) is this information stored?	What is the Legal Authority for collection of this information?	Does this system share PII externally? (please detail in question 9)
	<p>counseling and completion of required retirement/benefit forms. In addition, employees have direct access to their individual retirement and limited salary data through the Employee Benefit Center (EBC) for overall transparency and data integrity review. The Retirement uses a centralized database of federal personnel/payroll retirement and benefit data to perform calculation estimates for Federal retirement, Thrift Savings Plan annuity options, Social Security benefits, survivor benefits, death in service, military, and civilian</p>		<p>File Systems Records PBG-3: Employee Payroll, Leave and Attendance Records</p>	<p>Chapters 11, 33, and 63. 29 U.S.C. 1302; 44 U.S.C. 3101; 5 U.S.C. 301, and 5501-5584.</p>	

Name of component	Describe the component (1 or 2 sentences)	Does this component contain PII?	In what system of records (SORN) is this information stored?	What is the Legal Authority for collection of this information?	Does this system share PII externally? (please detail in question 9)
	<p>deposit service calculations. Facilitates management and filing of electronic forms for retirement application packages and civilian service history calculations (SCD). This module includes the Employee Benefit Center (EBC), which creates a secured self-portal to access a variety of information regarding retirement and benefit options, civilian service, and payroll history along with the ability to electronically complete federal personnel forms or upload documentation to elect benefits. EBC also provides access to retirement and</p>				

Name of component	Describe the component (1 or 2 sentences)	Does this component contain PII?	In what system of records (SORN) is this information stored?	What is the Legal Authority for collection of this information?	Does this system share PII externally? (please detail in question 9)
Employee & Labor Relations	<p>financial planning tools and literacy e-seminars.</p> <p>The Employee & Labor Relations module allows users to upload, process, and store all the documents related to an adverse action, conduct, or performance-based case. In addition, it tracks steps associated with the employee and labor relations process, from initial employee complaints to disciplinary actions.</p>	Yes	<p>OPM/GOVT-1 – General Personnel Records</p> <p>OPM/GOVT-2 – Employee Performance File System Records</p> <p>OPM/GOVT-3 – Records of Adverse Actions, Performance Based Reductions in Grade and Removal Actions, and Termination of Probationers</p> <p>PBGC- 23 – Internal Investigations of Allegations of Harassing Conduct</p>	<p>5 U.S.C. 301, 1301, 4303, 7504, 7514, 7543</p> <p>5 U.S.C. 1104, 3321, 4305, and 5405, and Executive Order 12107.</p> <p>5 U.S.C. 3321, 4303, 7504, 7514, and 7543.</p> <p>29 U.S.C. 1302; 44 U.S.C. 3101; 5 U.S.C. 301; 42 U.S.C. 2000e, et seq.</p>	No

Name of component	Describe the component (1 or 2 sentences)	Does this component contain PII?	In what system of records (SORN) is this information stored?	What is the Legal Authority for collection of this information?	Does this system share PII externally? (please detail in question 9)
			PBGC- 8 – Employee Relations Files OPM/GOVT-10 Employee Medical File Systems Records	29 U.S.C. 1302; 44 U.S.C. 3101; 5 U.S.C. 301; 5 U.S.C.7101; 42 U.S.C. 2000e et seq. Executive Orders 12107, 12196, and 12564 and 5 U.S.C. Chapters 11, 33, and 63.	

2.2 The System as a Whole

1. Please describe the purpose of the system when considered as a whole. Please include if this is an existing system (either an annual recertification update or a major change).

OMAFedRAMP consists of Software as a Service (SaaS) systems provided by certified Cloud Service Providers (CSP). FedHR Navigator is a child/subsystem of the OMAFedRAMP. FedHR Navigator is a FedRAMP authorized product provided by the CPS, Economic Systems Inc. (EconSys). The combined FedHR Navigator modules assist PBGC employees with retirement planning, financial literacy education, performance appraisals, performance improvement plans, and Employee & Labor Relations process tracking.

2. What is the Confidentiality, Availability, and Integrity ratings for the system as a whole?

Confidentiality	Moderate
Integrity	Moderate
Availability	Moderate

3. List and discuss the sources from which the system collects PII (for instance, from an individual, another federal agency, etc.), the format in which PII is collected (for instance, via a form, face-to-face, phone, etc.), the notification given at time of collection from an individual regarding the Privacy Act, and the ability to opt-out of collection (and the consequences of opting out). Include a copy of all forms and Privacy Act statements used to collect information.

PII contained in FedHR Navigator is mainly loaded manually via a file from OMAG2G HRMS.

During the new user registration process, employees provide their last name, birthday, and SSN that is obfuscated and used for the 2-tier identity verification purpose. Before employees enter this PII, the Privacy Act notification is provided online.

Please see Appendix A Privacy Act Notification from FedHR Navigator.

4. Discuss any privacy controls that PBGC inherits from an external provider (cloud provider, third party provider, another government agency, etc.). If an

Interconnection Security Agreement (ISA), Memorandum of Understanding (MOU), or similar document is in place, please summarize the privacy applicable portions of that document.

There is no applicable Service Level Agreement (SLA), ISA, or MOU for FedHR Navigator. OMAFedRAMP or FedHR Navigator does not inherit any privacy controls from EconSys. All privacy controls are implemented internally by OMA, Common Control Provider (CCP) Privacy Office, or other PBGC CCP.

5. For the user roles in the system:

Table 1: ePerformance

Role Name	Number of Users in that role	Approver	Access Level (Read, Write, etc.)	Recertification Date
Employees	986	Johane Pace	Read, Write	Not Applicable (federal employees are automatically granted a role upon hire; their ability to access the system is terminated upon their separation from PBGC)
Supervisor	205	Johane Pace	Read, Write	06/18/2024
Performance Liaison	20	Monica Proctor	Read, Write	06/18/2024
Performance Manager	11	Monica Proctor	Read, Write, Execute	06/18/2024

Table 2: Employee and Labor Relation

Role Name	Number of Users in that role	Approver	Access Level (Read, Write, etc.)	Recertification Date
ER/LR Super User	1	John McLemore	Read, Write	06/18/2024

ER/LR Specialist	1	LaShawn Dennis	Read, Write	06/18/2024
------------------	---	----------------	-------------	------------

Table 3: Retirement Calculation

Role Name	Number of Users in that role	Approver	Access Level (Read, Write, etc.)	Recertification Date
Administrator	4	Johane Pace	<i>Read, Write, Execute</i>	06/18/2024
Benefits Specialist	7	Johane Pace	<i>Read, Write, Execute</i>	06/18/2024
HR Specialist	14	Johane Pace	<i>Read, Write, Execute</i>	06/18/2024
Data Feed Specialist	1	Todd Smith	Execute	06/18/2024
Employees	986	Johane Pace	Read, Write	Not Applicable (federal employees are automatically granted a role upon hire; their ability to access the system is terminated upon their separation from PBGC)

6. Does the System leverage the Enterprise Access Controls?

- Yes
 No

7. Discuss the Physical, Technical, and Administrative controls that are employed to secure the PII in the system.

FedHR physical security controls employed to secure the PII in the system include:

1. Security guards
2. Key entry
3. Locked file cabinets
4. Secured facility
5. Identification badges
6. Locked offices

FedHR technical security controls employed to secure the PII in the system include:

1. Password protection
2. Virtual Private Network
3. Firewalls
4. Unique user identification names
5. Encryption
6. Intrusion Detection Systems
7. Personal Identity Verification (PIV) card access
8. Public Key Infrastructure (PKI) Certificates

FedHR administrative security controls employed to secure the PII in the system include:

1. Periodic security audits
2. Regular monitoring of user's activity
3. Annual refresher training for security, Privacy, and records management
4. Mandatory on-boarding training for security and Privacy and Records management personnel
5. Role-based training

OMAFedRAMP leverages the following controls from the vendor: Backups are secured off-site and security methods are employed to ensure that only authorized personnel have access to PII.

8. For the PII in the system, discuss the actual/intended uses of the PII, the steps taken to limit the PII collected to the minimum needed, and the reasons the PII is necessary and relevant.

FedHR PII will assist employees with financial/retirement planning and provide support for performance management and employee and labor relations processes.

To limit the collection of PII, HRD only utilizes the appropriate Federal and agency-specific forms and authorized supporting documentation for the collection of PII. HRD and Privacy personnel regularly review PBGC-specific forms for appropriate collection of PII. Privacy and HRD collaborate to minimize the collection of PII necessary to perform agency functions.

Note: SSNs, dates of birth, and last names are also used for user authentication. OMAFedRAMP users logging into the system must log in with unique identifiers. Multifactor authentication has been implemented and enabled and is required for all users logging into FedHR. PBGC has implemented CAC/PIV smartcard with a valid certificate. Users must correctly validate their unique pin for the cards.

Please note - FedHR is part of an ongoing IPT for HRMS systems. The current log-in requires input of several pieces of PII. In the interim, HRD has obfuscated the social security number and has submitted a request to the vendor to obfuscate the date of birth used on the log-in screen to these systems. HRD, Privacy, ECD, and ITIOD are currently working with the vendor to determine if there is an alternate method available to access the system that limits the use of employees' PII to register.

9. Discuss the data flows within the system (include sources of data for data flowing into the system, destinations for data flowing out of the system, and any routine uses applicable to the system). For any information that is shared internally, be sure to discuss whether these data interconnections are noted in CSAM. Be sure to include any MOU, ISA, or Interagency Agreements.

FedHR receives a manual upload from PBGC via a FTP-secured portal bi-weekly. Data is not shared externally or internally with any other system.

10. Does the system leverage the commonly offered control for Accounting of Disclosures?

- Yes
 No

11. If your system collects, Social Security Numbers:

- a. Please provide a justification for the collection, use, maintenance, and disposal of PII in the form of SSN?

FedHR utilizes the authority to solicit, collect, maintain and dispose of SSNs provided by law, require interoperability with organizations beyond PBGC to include Interior Business Center, U.S. Department of the Treasury, Office of Personnel Management, U.S. Department of Labor, Social Security Administration, Internal Revenue System, law enforcement offices, and other federal, state, and local entities.

Until a reasonable alternative exists for collection of data other than the SSN, such as cross-wide reference or employee identification number, system decommission or changes, or federal-wide changes that eliminate the need for SSN use, HRD will require the indefinite use of SSNs. FedHR internal standard operating procedures and communications will be reviewed annually to ensure data is afforded the highest protections practicable through use of appropriate administrative, technical, and physical safeguards.

Cited Sources For Data, PII, and SSN Collection:

• *Public Law 104-134 (April 26, 1996) requires that any person doing business with the Federal Government furnish SSN or TIN, 2) E.O 9397 as amended by E.O. 13478 (November 18, 2008); 3) 5 U.S.C 301; 4) 31 USC Chapter 3511, 3512, 3513; 5) Federal Employee Retirement Law (Chapter 84, Title 5 US Code; 6) the Federal Retirement Group Life Insurance Law (Chapter 87, Title 5 US Code); 7) the Federal Health Benefits Law (Chapter 89, Title 5 US Code); 8) Civil Service Retirement Law (Chapter 83, subchapter iii, Title 5 US Code); 9) Veterans Preference Act 1944; 10) Internal Revenue Code sections 3402(f)(2) and 6109; 11) Privacy Act System of Records Notice (SORN), OPM/CENTRAL 1 Civil Service Retirement and Insurance; 12) Federal Employees Compensation Act 5 U.S.C. 8101; Debt Collection Act; 13) Section 6303 of 5 U.S.C., "Annual Leave Accrual," authorizes collection of information to determine and record service that may be creditable for accrual of annual leave. 14) Part 351.503, 5 C.F.R., "Length of Service," authorizes collection of data to determine and record service that may be creditable for reduction-in-force retention purposes.*

- b. Under which authorized uses, as described in the “Reduction of Use of Social Security Numbers (SSN) in PBGC” policy document?

According to the PBGC Corporate Social Security Numbers (SSN) Reduction Policy, the justification for collection, use, maintenance, and disposal of PII in the form of SSN is:

e. Administration of Federal Worker’s Compensation. The Federal Worker’s Compensation Program continues to track individuals through the use of the SSN. In addition, OPM continues to track Federal employees through the use of the SSN. Thus, systems, processes, or forms that interact with or provide information for the administration of these types of systems or associated systems may be required to retain the SSN.

- c. If the answer to b., above, is “Compelling Business Need,” please provide a plan to reduce the use of SSNs, highlighting activities that can be completed in the next 12 months.

N/A

2.3 Privacy Office Review

Name of Reviewer	William Black
Date Reviewed	08/28/2024
Expiration Date	8/27/2025
Result	<input checked="" type="checkbox"/> Approved without conditions <input type="checkbox"/> Approved with conditions (see below). <input type="checkbox"/> Denied

(For Privacy Office Use Only)

Discuss analysis of risks and compensating controls (or other mitigation steps.

Not Applicable

Discuss any conditions on Approval.

Not Applicable

3 Appendix A Privacy Act Notification from FedHR Navigator

USE OF THIS OR ANY OTHER GOVERNMENT INTEREST COMPUTER SYSTEM CONSTITUTES YOUR CONSENT TO MONITORING BY AUTHORIZED AGENCY PERSONNEL FOR COMPUTER SECURITY AND SYSTEM MANAGEMENT PURPOSES. THIS SYSTEM AND ALL RELATED EQUIPMENT ARE TO BE USED FOR THE COMMUNICATIONS, TRANSMISSION, PROCESSING, MANIPULATION, AND STORAGE OF OFFICIAL U.S. GOVERNMENT OR OTHER AUTHORIZED INFORMATION ONLY. UNAUTHORIZED USE OF THIS COMPUTER MAY SUBJECT YOU TO CRIMINAL PROSECUTION AND PENALTIES.

Privacy Act Notice

We are authorized to request PRIVACY ACT information under 3 CFR 13478 - Executive Order 13478 of November 18, 2008 authorizes us to ask for your Social Security number, which will be used to identify your account. We will use the information you provide to process the transaction you request on the Web site. This information may also be shared with other Federal agencies to administer your account or for statistical, auditing, or archiving purposes. In addition, we may share the information with law enforcement agencies investigating, prosecuting, or enforcing a violation of civil or criminal law or with other agencies for the purpose of implementing a statute, rule, or order. You are not required by law to provide this information, but if you do not provide it, it may not be possible to process the actions you request on this Web site.