Privacy Impact Assessment (PIA)
for the

Government Retirements and Benefits
May 27, 2022

For PIA Certification Updates Only: This PIA was reviewed on [Enter date] by [Name of reviewer] certifying the information contained here is valid and up to date.

Contact Point

Contact Person/Title: Qiana Gray, Information Systems Human Resources Specialist  
Contact Email: Qiana.gray@ed.gov

System Owner

Name/Title: Qiana Gray, Information Systems Human Resources Specialist  
Principal Office: Qiana.gray@ed.gov

Please submit completed Privacy Impact Assessments to the Privacy Office at privacysafeguards@ed.gov

FY 2020
Please complete this Privacy Impact Assessment (PIA) on how personally identifiable information (PII) is collected, stored, protected, shared, and managed electronically by your system. You may wish to consult with your ISSO in completing this document. If a question does not apply to your system, please answer with N/A.

1. Introduction

1.1. Describe the system including the name, acronym, and a brief description of the program or purpose for the system.

The U.S. Department of Education’s (Department’s) Office of Human Resources (OHR) procured the Government Retirement and Benefits (GRB) system to perform accurate retirement calculations for new and existing Department employees. Prior to procuring this solution, human resources (HR) specialists would manually calculate these values, leading to a greater potential for miscalculations. GRB was identified and procured to reduce the potential for these incorrect calculations. GRB is a web-based software-as-a-service (SaaS) federal retirement and benefits solution provided to the Department and administered for maintenance purposes by Government Retirement & Benefits, Inc (GRB, Inc).

GRB allows for the calculation of Federal employee retirement benefit estimates, disability and death benefit estimates, service computation date calculation, military/civilian deposit and redeposit requirements, and retirement plan determination. The application can also prepopulate U.S. Office of Personnel Management (OPM) Standard Forms (SFs) on behalf of the employee for submission for retirement benefits. Employee information such as Social Security numbers (SSNs) are collected for the purpose of generating OPM SFs required for retirement processing on behalf of the employee for submission to the OPM. GRB will add the employee’s data (such as name, SSN, date of birth, etc.) to the retirement form once the calculations have been performed. Once a form is generated, the employee is responsible for reviewing and confirming information in the form prior to the HR specialist submission to OPM for processing. The Federal employee then reviews documents or information provided by the HR specialist. A final review to validate PII is performed by the HR specialist before submission to the Department of Interior (DOI) for additional payroll related processing, and then forwarded to OPM on behalf of the employee.

GRB is currently only accessible by approved HR specialists and data is entered into the system on two occasions:
1. Perform retirement benefits calculations when a new Department hire either transfers from another federal agency or has prior federal service. The HR
specialist creates a profile for this employee to assist in the calculation of the employee’s service computation date.

2. Perform retirement benefits calculations that are requested by current Department employees. The data to perform these functions is gathered by the HR specialist by reviewing documents contained within the employee’s Official Personnel File (eOPF), including the SF-50 and other personnel-related documentation.

Access to the application is managed by the branch chief or authorized delegate, Benefits and Work/Life Branch within OHR. Information retrieval is only done by employee name. No other identifiers are used as part of the retrieval process. Information contained within GRB is not shared with any other systems.

1.2. Describe the purpose for which the personally identifiable information (PII)\(^1\) is collected, used, maintained or shared.

The purpose of collecting this information is to: (1) assist Department employees on determining retirement eligibility and benefits the employee would be eligible to receive upon retirement, and (2) pre-populate required OPM forms to support retirement processing requests.

1.3. Is this a new system, or one that is currently in operation?

**Currently Operating System**

1.4. Is this PIA new, or is it updating a previous version?

**New PIA**

New guidance on how to apply the definition of PII required that a PIA be completed for the system.

1.5. Is the system operated by the agency or by a contractor?

**Contractor**

\(^1\) The term “personally identifiable information” refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. **OMB Circular A-130, page 33**
1.5.1. If the system is operated by a contractor, does the contract or other acquisition-related documents include privacy requirements?

☐ N/A

Yes

2. Legal Authorities and Other Requirements

If you are unsure of your legal authority, please contact your program attorney.

2.1. What specific legal authorities and/or agreements permit and regulate the collection and use of data by the system? Please include name and citation of the authority.


SORN

2.2. Is the information in this system retrieved by an individual’s name or personal identifier such as a Social Security Number or other identification?

☐ Yes

Information in the system is retrieved by the federal employee’s name.

2.2.1. If the above answer is YES, this system will need to be covered by Privacy Act System of Records Notice(s) (SORN(s)).\(^2\) Please provide the SORN name, number, Federal Register citation and link, or indicate that a SORN is in progress.

☐ N/A


2.2.2. If the above answer is NO, explain why a SORN was not necessary. For example, the information is not retrieved by an identifier, the information is not maintained in a system of records, or the information is not maintained by the Department, etc.

\(^2\) A System of Records Notice (SORN) is a formal notice to the public that identifies the purpose for which PII is collected, from whom and what type of PII is collected, how the PII is shared externally (routine uses), and how to access and correct any PII maintained by ED. [https://connected.ed.gov/om/Documents/SORN-Process.pdf](https://connected.ed.gov/om/Documents/SORN-Process.pdf)
Records Management
If you do not know your records schedule, please consult with your records liaison or send an email to RMHelp@ed.gov

2.3. What is the records retention schedule approved by National Archives and Records Administration (NARA) for the records contained in this system? Please provide all relevant NARA schedule numbers and disposition instructions.

In accordance with GRS 2.5 Employee Separation Records, item 020 Individual employee separation case files, records are considered temporary and should be destroyed one year after date of separation or transfer, but longer retention is authorized if required for business use.

2.4. Is the PII contained in this system disposed of appropriately, and in accordance with the timelines in the records disposition schedule?

Yes

3. Characterization and Use of Information

Collection
3.1. List the specific PII elements (e.g., name, email, address, phone number, date of birth, Social Security, etc.) that the system collects, uses, disseminates, or maintains.

The system collects data on Department employees and their dependents/spouses to support retirement claims processing and benefit estimations.

Mandatory data includes the following data:

- Employee name, gender, Social Security number (SSN), employee date of birth, appointment date (employee’s current federal appointment date beginning at the Department), service type (Military, Law Enforcement, Civilian, etc.), retirement system (Civil Service Retirement System [CSRS] or Federal Employees Retirement System [FERS]), work schedule (full-time or part-time), current pay basis (hourly, annually, etc.), current pay rate (rate based on Current Pay Basic), current pay effective date, sick and annual leave balances, Federal Employee Group Life Insurance (FEGLI) plan code, Federal Employees Health Benefits (FEHB) plan code, and dental and vision monthly premiums.
While the system has the capability to include the additional personal information fields shown below, the fields are only completed if there should be a death of an employee and the HR specialist is working with the employee’s designated beneficiary or if the employee requests the additional data be added to calculations:

- Beneficiary name, date of birth, gender, home phone number, alternate phone number, mailing address, country, country code, postal code, personal email address, marriage status, SSN, name, date of marriage, place of marriage, employee position description, employee leave accrual information, and number of dependent children.

Department employees and contractors have access to the system in order to perform the duties noted above. Information collected from these individuals include name, email address, username and password.

3.2. Does the system collect only the minimum amount required to achieve the purpose stated in Question 1.2?

Yes

The PII collected and maintained is the minimum amount required by GRB to assist with retirement eligibility, benefit estimation and the prepopulation of required OPM forms for retirement benefits.

3.3. What are the sources of PII collected (e.g., individual, school, another agency, commercial sources, etc.)?

The PII is collected via federal employee submission of the “Request For Retirement Estimate” form (ED-HR 2828) and existing employee files that have been loaded into the employee’s eOPF, including the SF-50 and other personnel-related documentation.

3.4. How is the PII collected from the stated sources listed in Question 3.3 (e.g., paper form, web page, database, etc.)?

Information comes from the federal employee if they have filled out a “Request for Retirement Estimate” form and documents contained within the employee’s eOPF, including the SF-50 and other personnel-related documentation.
3.5. How is the PII validated or confirmed to ensure the integrity of the information collected? Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

The PII is validated by the HR specialist upon initial receipt. The federal employee then reviews documents or information provided by the HR specialist. A final review to validate PII is performed by the HR specialist before submission to the DOI for additional payroll related processing, and then forwarded by DOI to OPM, on behalf of the employee.

Use

3.6. Describe how the PII is used to achieve the purpose stated in Question 1.2 above.

The system collects information on Department employees to assist with retirement eligibility, benefit estimation, and the prepopulation of required OPM forms for retirement benefits.

3.7. Is the system using PII for testing/researching new applications or information systems prior to deployment or for training employees?

No

3.7.1. If the above answer is YES, what controls are in place to minimize the risk and protect the data?

✓ N/A

Social Security Numbers

It is the Department’s Policy that, in order to collect Social Security Numbers, the System Owner must state the collection is: 1) authorized by law, 2) necessary for an agency purpose, and 3) there is no reasonable alternative.

3.8. Does the system collect Social Security Numbers? Note that if the system maintains Social Security Numbers but does not explicitly collect them, answer 3.8.1 to address the purpose for maintaining them.

Yes

---

3 Examples include restricted form filling, account verification, editing and validating information as it’s collected, and communication with the individual whose information it is.
3.8.1. If the above answer is **YES**, explain the purpose for its collection, and how the SSN will be used.

- [ ] N/A

The Social Security number is required in order to complete the federal employee’s retirement forms to send to OPM for processing.

3.8.2. Specify any alternatives considered in the collection of SSNs and why the alternatives were not selected.

- [ ] N/A

There were no alternatives considered as SSN is required for submission per OPM requirements.

4. **Notice**

4.1. How does the system provide individuals with notice about the collection of PII prior to its collection (e.g., direct notice, such as a Privacy Act Statement (if applicable) or public notice, such as a SORN, PIA)? If notice is not provided, explain why not.

A Privacy Act Statement is included on the “Request for Retirement Estimate” form that the federal employee submits and sends to Human Resources Work/Life Team for processing.

4.2. Provide the text of the notice or the link to the webpage where the notice is posted if notice is provided other than by SORN or PIA.

- [ ] N/A

**Authorities:** Calculating retirement benefits and tracking retirement applicant cases requires collecting PII. The authorities for maintaining personnel information are 5 United States Code (U.S.C.) 1302, 2951, 3301, 3372, 4118, 8339, 8347, and 8415 and Executive Orders (E.O.) 9397, as amended by 13478, 9830, and 12107. Authorities recording Social Security Numbers are E.O. 9397, 26 CFR 31.6011(b)–2, and 26 Code of Federal Regulations (CFR) 31.6109–1.

**Purpose:** The purpose of collecting this information is to provide accurate service computation dates and retirement estimates to Department employees.

**Disclosures:** The information will not be disclosed outside the Office of Finance and Operations until it is sent to the U.S. Office of Personnel Management (OPM) for
retirement processing. The completed retirement package is forwarded by the HR specialist to the Department of Interior (DOI) for additional payroll related processing, and then forwarded by DOI to OPM, on behalf of the employee.

**Consequences of Failure to Provide information:** Failure to provide this information will result in an inability to provide accurate retirement calculations.

Additional information about this system can be found in the Privacy Impact Assessment.

4.3. What opportunities are available for individuals to consent to uses (including new uses of previously collected PII), decline to provide PII, or opt out of the project?

Employees have the opportunity to not submit PII on the “Request for Retirement Estimate” form but not doing so may delay or deter the employee’s retirement processing.

4.4. Is the notice referenced in Question 4.1 reviewed and revised when there are changes in the practice, policy, or activities that affect the PII and privacy to ensure that individuals are aware of and can consent to, where feasible, these changes?

Yes

5. **Information Sharing and Disclosures**

**Internal**

5.1. Will PII be shared internally with other ED principal offices? If the answer is NO, please skip to Question 5.4.

No

5.2. What PII will be shared and with whom?

✔️ N/A

5.3. What is the purpose for sharing the specified PII with the specified internal organizations?

✔️ N/A

**External**

5.4. Will the PII contained in the system be shared with external entities (e.g. another agency, school district, the public, etc.)? If the answer is NO, please skip to Question 6.1.
Yes

The information will not be disclosed outside the Office of Finance and Operations until it is sent to the OPM for retirement processing. The completed retirement package is forwarded by the HR specialist to the DOI for additional payroll related processing, and then forwarded by DOI to OPM, on behalf of the employee.

5.5. What PII will be shared and with whom? List programmatic disclosures only.\(^4\)

\textbf{Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose.}

\begin{itemize}
  \item N/A
\end{itemize}

The PII mentioned in Section 3.1 will be shared with DOI and OPM for the respective agencies to process the federal employee’s retirement paperwork.

5.6. What is the purpose for sharing the PII with the specified external entities?

\begin{itemize}
  \item N/A
\end{itemize}

It is required in order to process the federal employee’s retirement paperwork.

5.7. Is the sharing with the external entities authorized?

\begin{itemize}
  \item N/A
  \item Yes
\end{itemize}

5.8. Is the system able to provide and retain an account of any disclosures made and make it available upon request?

\begin{itemize}
  \item N/A
  \item No
\end{itemize}

5.9. How is the PII shared with the external entity (e.g., email, computer match, encrypted line, etc.)?

\begin{itemize}
  \item N/A
\end{itemize}

Retirement documents are sent from ED to the payroll processor, the DOI, via United Parcel Service (UPS) or DOI’s Secure Transport Portal. DOI then forwards the retirement documents to OPM.

\(^4\) If this information is covered by Privacy Act System of Records Notice (SORN) please list only relevant programmatic disclosures listed under the Routine Uses section.
5.10. Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or other type of approved sharing agreement with another agency?

☑ N/A

Click here to select.

5.11. Does the project place limitation on re-disclosure?

☑ N/A

Click here to select.

6. Redress

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

Federal employee information is maintained in their eOPF and they are able to access it when they are on the Department network.

In addition, individuals wishing to request access to their records can contact the appropriate OPM or Department office, as specified in the Notification Procedure section. Individuals must furnish the following information for their records to be located and identified: a. Full name(s). b. Date of birth. c. Social Security number. d. Last employing agency (including duty station) and approximate date(s) of employment (for former Federal employees). e. Signature. Individuals requesting access must also comply with the Office's Privacy Act regulations on verification of identity and access to records (5 CFR part 297).

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

Current employees wishing to request amendment of their records should contact call or email Human Resources, Work/Life. Former employees should contact the system manager listed in the SORN referenced in question 2.2.1. Individuals must furnish the following information for their records to be located and identified. a. Full name(s). b. Date of birth. c. Social Security number. d. Last employing agency (including duty station) and approximate date(s) of employment (for former Federal employees). e. Signature. Individuals requesting amendment must also comply with the Office's Privacy Act regulations on verification of identity and amendment of records (5 CFR part 297).
6.3. How does the project notify individuals about the procedures for correcting their information?

The system of records notice listed in question 2.2 explains the procedures for correcting customer information.

7. Safeguards

If you are unsure which safeguards will apply, please consult with your ISSO.

7.1. Does the principal office work with their CSO/ISSO to build privacy & security into the system and build privacy extensions to the extent feasible?

[Yes]

7.2. Is an Authority to Operate (ATO) required?

[Yes]

7.3. Under NIST FIPS Pub. 199, what is the security categorization of the system: Low, Moderate, or High?

☐ N/A

[Moderate]

7.4. What administrative, technical, and physical safeguards are in place to protect the information?

The GRB system is hosted outside the Department’s network by a vendor that is currently pursuing FedRAMP certification. The system is provided as a Software as a Service (SaaS) and is required to complete routine testing of their environment to ensure the confidentiality, integrity, and availability of the information in the system and services provided. The CSP enforces security controls over the physical facility where the system is hosted in adherence with FedRAMP standards.

The GRB system utilizes role-based authentication to ensure only authorized users can access information, and they can only access the information needed to perform their duties. Authentication to the server is permitted only over secure, encrypted connections.

7.5. Is the information in the system appropriately secured in accordance with the IT security requirements and procedures as required by Federal law and policy?
7.6. Has a risk assessment been conducted where appropriate security controls to protect against that risk have been identified and implemented?

Yes

7.7. Please describe any monitoring, testing or evaluation conducted on a regular basis to ensure the security controls continue to work properly at safeguarding the PII.

The GRB cloud service provider performs monitoring, testing, and evaluation of their software. The cloud service provider is responsible for ensuring access controls are working as defined in the software.

The following tasks are performed to safeguard GRB information:

- Monthly vulnerability scan as required by FedRamp
- Annual contingency plan test performed as required by FedRamp
- Annual self-assessments conducted; and/or annual security assessments performed by the Department Security Authorization Team
- Annual updates to system security documents
- Annual mandatory Cybersecurity and Privacy Training for employees and contractors

8. Auditing and Accountability

8.1. How does the system owner assess and ensure that the PII is used in accordance with stated practices in this PIA?

The system owner ensures that the GRB administrator completes reviews of user accounts on a regular basis to ensure access is limited to only authorized individuals. The system owner works with the Department’s Privacy Office to complete a PIA and to ensure the PIA is accurate and updated as required. The system owner also completes the Department Risk Management Framework process to secure an ATO. The system owner works with individuals who have access to ensure the system is being used appropriately and in accordance with the practices detailed in this document.

8.2. Does the system owner continuously monitor and audit the privacy controls to ensure effective implementation?
8.3. What are the privacy risks associated with this system and how are those risks mitigated?

Privacy risks associated with GRB include unencrypted data being transmitted, lost, stolen, or compromised. Data breaches involving PII are potentially hazardous to both individuals and organizations. Individual harm may include identity theft, embarrassment, or financial loss. Organizational harm may include a loss of public trust, legal liability, or remediation costs.

The risks are mitigated by the above-mentioned safeguards, limiting access to only those with a legitimate need to know, and working closely with the security and privacy staff at the Department. To further mitigate this risk, the following safeguards have been implemented:

- Monthly vulnerability scans
- Annual contingency plan test
- Annual or ongoing security assessments
- Annual cybersecurity and privacy training for GRB users

Risks are also mitigated by updating security patches and updating devices operating software, amongst other software. Scans are run on the production environment each month in support of the monthly patching cycle. Collecting the minimum PII necessary to achieve the system’s purpose also mitigates privacy risks.