



Privacy Impact Assessment for
Government Retirement Benefits
(GRB)

August 12, 2022

Contact Point

Joy Fisher

Supervisor, Benefits & Work-Life Programs
OPM Human Resources

Reviewing Official

Kellie Cosgrove Riley
Chief Privacy Officer



Abstract

The Government Retirement Benefits platform (GRB) is a contracted Federal Retirement Administration Software as a Service enterprise system that is used by Office of Personnel Management (OPM) Human Resources to provide benefit and retirement computations to OPM employees. GRB provides OPM employees on-demand access to their benefits, retirement computation tools, and total compensation awareness. It also provides OPM HR Benefits Specialists with a dashboard to populate employees creditable service and input details to compute and prepare retirement estimate reports, military deposits, civilian deposits, survivor benefits, disability retirement, severance pay, and service computation dates. This Privacy Impact Assessment is being completed because GRB contains personally identifiable information.

Overview

The Government Retirement Benefits platform (GRB) is a contracted Federal Retirement Administration Software as a Service enterprise system that is used by Office of Personnel Management (OPM) Human Resources to provide benefit and retirement computations to OPM employees. GRB is comprised of a suite of tools that OPM Human Resources staff use to conduct a variety of tasks such as retirement related computations, service computation date calculations, civilian deposits and redeposits, military deposits, survivor benefits, and severance pay computations. The GRB platform also permits OPM HR staff to submit retirement forms and manage retirement cases and provides access to all retirement and benefit standard forms. GRB streamlines an otherwise manual computation process for OPM HR staff, increasing productivity and vastly reducing potential errors. OPM employees can also access and use GRB to review their own information. For example, OPM employees may review their total compensation and use the self-calculator to determine their retirement eligibility dates. Additionally, the GRB Platform contains various resources and tools for employees such as



benefit program fact sheets, informational videos, access to standard forms, and options to submit retirement applications forms to OPM Human Resources. GRB is populated with information about OPM employees from the HR Links system. The following information from HR Links is captured to populate OPM employees' GRB profile and to compute an estimate of retirement benefits: employee's name, date of birth, gender, Social Security number, address, military service (if applicable), salary, work schedule, and leave balances. Access to employee profiles in GRB is restricted to those OPM Human Resources staff that require access to conduct computations. In addition, every OPM employee can access their own information by registering for a GRB account. A GRB profile is created for every OPM employee even if they do not register for an account.

Section 1.0. Authorities and Other Requirements

1.1. What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

In general, OPM collects information about its employees to conduct its human resources management functions pursuant to a variety of statutory provisions contained in Title 5 of the United States Code and processes and calculates retirement information in accordance with the provisions of 5 U.S.C. Chapters 83 and 84. Social Security numbers are collected and used in accordance with Executive Order 9397, as amended by Executive Order 13478.

1.2. What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

OPM GOVT -1, General Personnel Records, and OPM Internal-5, Pay, Leave, and Travel Records.



1.3. Has a system security plan been completed for the information system(s) supporting the project?

No, the cloud service provider has a FEDRAMP approved FIPS-199 compliant system security plan (SSP). A specific OPM SSP is in process with a projected completion date in August 2022.

1.4. Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes. Records in GRB are subject to GRS 5.2.

1.5. If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The information in GRB is not collected from or about members of the public, therefore the PRA does not apply.

Section 2.0. Characterization of the Information

2.1. Identify the information the project collects, uses, disseminates, or maintains.

The following information about OPM employees is collected, used, disseminated, or maintained in GRB: employee name, date of birth, Social Security number, gender, Employment Information (Salary, Schedule, Service Computation Date, Military Service), and (6) address.

2.2. What are the sources of the information and how is the information collected for the project?

An HR Specialist manually updates or populates GRB every pay period using data from the HR Links system.



2.3. Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

GRB does not collect publicly available information or information from commercial sources.

2.4. Discuss how accuracy of the data is ensured.

The information in GRB is populated from HR Links, where information is regularly reviewed and updated as routine personnel actions are conducted and documented by an SF-50. OPM Human Resources specialists review and cross reference information available from a variety of systems primarily eOPF to ensure accuracy of information uploaded to GRB.

2.5. Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that more information than is necessary to achieve the business purpose of GRB will be loaded into the system.

Mitigation: This risk is mitigated in the structure of GRB, which is designed with pre-established fields to collect only information necessary for the GRB employee profile and reporting options.

Privacy Risk: There is a risk that the information in GRB may be inaccurate and result in a miscalculation of benefit information.

Mitigation: This risk is mitigated by populating GRB from trusted and verified sources and by OPM HR staff verifying the employee data in GRB when they are calculating benefits.

Section 3.0. Uses of the Information

3.1. Describe how and why the project uses the information.

Employee information is uploaded to GRB to allow employees to see a comprehensive review of their benefits, utilize the self-calculating retirement



computation option, pre-fill retirement related forms, and submit retirement applications. The GRB suite of tools assists OPM HR Specialists with completing accurate service computation date reports, retirement estimates, civilian and military deposit reports, severance pay, death benefits, disability retirement estimates, voluntary retirement estimates, and retirement application forms.

3.2. Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how OPM plans to use such results.

The system does not use technology to conduct electronic searches, queries, or analysis to discover predictive patterns or anomalies.

3.3. Are there other programs or offices with assigned roles and responsibilities within the system?

No, only select OPM Human Resources Specialists are assigned roles and responsibilities within GRB. Employees only have access to view their individual records and can insert varying retirement dates (which are not retained in GRB) to compute estimated benefits based off the chosen retirement date.

3.4. Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that unauthorized individuals will have access to the information in GRB or that authorized individuals will access the system for an unauthorized purpose.

Mitigation: This risk is mitigated by implementing strict protocols and procedures for individuals to obtain access and limiting that access consistent with their assigned roles. In addition, this risk is mitigated by only credentialing select HR employees the ability to upload data to GRB and blocking others from access and through audit functions. The OPM HR Specialist will upload the file to a secured GRB provided drop site for pick up/processing by the GRB system. This will update the employee information



to include current salary, benefit elections, and leave balances. Employees are only able to access their own information using their OPM work email address as the user id and a password that they create based on GRB security protocol of at least eight characters consisting of upper- and lower-case letters, at least one number and at least one special character. Once employees are separated from OPM their opm.gov account is deleted ending their access to an OPM email account which automatically ends access to GRB.

Section 4.0. Notice

4.1. How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

OPM employees receive general notice at the time their personnel information is collected concerning the reason for the collection and the purposes for which their information will be used. OPM Human Resources notifies employees during onboarding, bi-annual retirement seminars, and occasionally highlighted in the monthly Benefits and Work-Life publication. Notice is also provided through the publication of this PIA.

4.2. What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

OPM employees are not privileged to consent or deny the systematic upload of their basic profile information into GRB, however; employees can only access their retirement calculations by creating a GRB account. Upon creation of a GRB account employees have the ability to add additional information for the purpose of estimating retirement benefits.

4.3. Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals may not be aware that their information will be placed in GRB and accessed and used for various personnel reasons related to retirement benefits calculations.



Mitigation: This risk is not fully mitigated. Individuals receive general notice about the use of their personnel records at the time the information is collected, and this PIA provides some notice as well. In addition, some employees are told about GRB during the onboarding process or during training sessions.

Section 5.0. Data Retention by the Project

5.1. Explain how long and for what reason the information is retained.

The information in GRB is updated every two weeks and an employee's GRB profile is deleted one year after the employee separates from OPM. GRB profiles for current OPM employees will be retained for as long as OPM has an active license with GRB. Internal procedures are in place to remove an OPM employee's GRB profile once they are no longer an active OPM employee.

5.2. Privacy Impact Analysis: Related to Retention.

Privacy Risk: There is a risk that information in GRB will be retained for longer than is necessary for its intended purpose.

Mitigation: This risk is mitigated through internal procedures by which information about separated employees is deleted from GRB one year after separation.

Section 6.0. Information Sharing

6.1. Is information shared outside of OPM as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Information is shared with the GRB vendor as authorized by the contract between OPM and GRB and OPM GOVT -1, General Personnel Records.



6.2. Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

The disclosure of information to the GRB contractor is done pursuant to routine use in the OPM GOVT-1 SORN and is consistent with the purpose for which the information was originally collected, as articulated in that SORN, which is, in part, to determine an employee's status, eligibility, and rights to benefits.

6.3. Does the project place limitations on re-dissemination?

The contract between OPM and GRB prohibits the GRB contractor from disseminating GRB information to anyone other than an employee accessing their specific file.

6.4. Describe how the project maintains a record of any disclosures outside of OPM.

All information accessed, provide to, or retrieved from GRB is audited. The audit logs include who accessed or retrieved the information, when the information was accessed or retrieved and what the information included. OPM can gain access to the contractor's audit log at any time upon request.

6.5. Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that the information will be disclosed and used for a purpose that is not consistent with the purposes for which it was originally collected.

Mitigation: This risk is mitigated by the terms of the agreement with the GRB vendor, which prohibits re-dissemination of the information in GRB. It is also mitigated through the audit logs from system audits that OPM may request as necessary in order to determine whether information is only being accessed by authorized users for an authorized purpose.



Section 7.0. Redress

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

Current OPM employees may register as a new user with their official OPM email address and by creating a password. They are provided with the OPM GRB license number to complete this registration process.

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

Individuals cannot update information within GRB. The information used to populate GRB is from the employee's official personnel record. If there are any discrepancies, the employee may contact OPM HR for assistance or may follow the procedure set out in the applicable SORN referenced in Section 1.2.

7.3. How does the project notify individuals about the procedures for correcting their information?

Information is provided to the employees during counseling sessions and there is a thorough review of the information provided based on GRB computations. Should the employee have any additional concerns or requests that information be changed, OPM HR can assist in resolving the issue. Employees also receive notice concerning how to correct inaccurate information via the relevant SORN identified in Section 1.2.

7.4. Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that an OPM employee will not be able to access their information in GRB and/or won't be able to correct erroneous information contained in their GRB profile.

Mitigation: This risk is mitigated through OPM HR providing employees with the information necessary to access their profiles in GRB and by assisting individuals when incorrect information is discovered.



Section 8.0. Auditing and Accountability

8.1. How does the project ensure that the information is used in accordance with stated practices in the PIA?

GRB employs a variety of security measures designed to ensure that information is not inappropriately disclosed or released. In addition, system audits are performed to ensure that information is being accessed and retrieved appropriately.

8.2. Describe what privacy training is provided to users either generally or specifically relevant to the project.

All OPM employees receive annual IT Security & Privacy Awareness Training, which covers the proper handling of PII. OPM employees accessing the system to view entitlements are not required to take any specific training.

8.3. What procedures are in place to determine which users may access the information and how does the project determine who has access?

All active OPM employees have a GRB profile based on the information from their official personnel record, which is constructed by OPM Human Resources staff members. The GRB Administrator is the OPM HR Benefits Officer who determines which OPM HR staff require access to GRB, based on the staff member's assigned tasks. Access to the system is removed when the HR Staff member is no longer in a position that requires access to GRB.

8.4. How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within OPM and outside?

Any new access to GRB or new information usage requirements will be evaluated by the appropriate HR personnel in consultation with relevant OPM stakeholders, including the Chief Information Security Officer, the Chief Privacy Officer, and the Office of the General Counsel.



Responsible Officials

Joy Fisher

Supervisory, Human Resources Specialist/GRB Administrator

Tyshawn Thomas

Chief Human Capital Officer

Approval Signature

Signed Copy on file with Chief Privacy Officer

Kellie Cosgrove Riley

Chief Privacy Officer