



GRB - Government Retirement Benefits

Privacy Impact Assessment

08/20/2019

POINT of CONTACT

Richard Speidel

Chief Privacy Officer

GSA IT

1800 F Street, NW

Washington, DC 20405

Table of contents

SECTION 1.0 PURPOSE OF COLLECTION

- 1.1 Why is GSA collecting the information?
- 1.2 What legal authority and/or agreements allow GSA to collect the information?
- 1.3 Is the information searchable by a personal identifier, for example a name or Social Security number? If so, what Privacy Act System of Records Notice(s) applies to the information being collected?
- 1.4 Has any information collection request (ICR) been submitted to or approved by OMB? If yes, provide the relevant names, OMB control numbers, and expiration dates.
- 1.5 Has a records retention schedule been approved by the National Archives and Records Administration (NARA) for the information system(s)? Explain how long and for what reason the information is retained.
- 1.6 Are there any privacy risks for this system that relate to the purpose of the collection? If so, how will GSA mitigate these risks?

SECTION 2.0 OPENNESS AND TRANSPARENCY

- 2.1 Will individuals be given notice prior to the collection and/or sharing of personal information about them? If not, please explain.
- 2.2 Are there any privacy risks for this system that relate to openness and transparency? If so, how will GSA mitigate these risks?

SECTION 3.0 DATA MINIMIZATION

- 3.1 Whose information is included in the system?
- 3.2 What PII will the system include?
- 3.3 Why is the collection and use of the PII necessary to the project or system?
- 3.4 Will the system create or aggregate new data about the individual? If so, how will this data be maintained and used?
- 3.5 What controls exist to protect the consolidated data and prevent unauthorized access?
- 3.6 Will the system monitor members of the public, GSA employees or contractors?
- 3.7 What kinds of report(s) can be produced on individuals?
- 3.8 Will the data included in any report(s) be de-identified? If so, what process(es) will be used to aggregate or de-identify the data?
- 3.9 Are there any privacy risks for this system that relate to data minimization? If so, how will GSA mitigate these risks?

SECTION 4.0 LIMITS ON USES AND SHARING OF INFORMATION

- 4.1 Is the information in the system, application or project limited to only the information that is needed to carry out the purpose of the collection?

4.2 Will GSA share any of the information with other individuals , Federal and/or state agencies, or private sector organizations? If so, how will GSA share the information?

4.3 Is the information collected directly from the individual or is it taken from another source? If so, what is the other source(s)?

4.4 Will the system, application or project interact with other systems, either within GSA or outside of GSA? If so, what other system(s), application(s) or project(s)? If so, how? If so, is a formal agreement(s) in place?

SECTION 5.0 DATA QUALITY AND INTEGRITY

5.1 How will the information collected be verified for accuracy and completeness?

5.2 Are there any privacy risks for individuals whose information is collected or used by the system, application or project that relate to data quality and integrity? If so, how will GSA mitigate these risks?

SECTION 6.0 SECURITY

6.1 Who or what will have access to the data in the project? What is the authorization process for access to the project?

6.2 Has GSA completed a system security plan for the information system(s) supporting the project?

6.3 How will the system be secured from a physical, technological, and managerial perspective?

6.4 Are there mechanisms in place to identify security breaches? If so, what are they?

6.5 Are there any privacy risks for this system that relate to security? If so, how will GSA mitigate these risks?

SECTION 7.0 INDIVIDUAL PARTICIPATION

7.1 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project? If no opportunities are available to consent, decline or opt out, please explain.

7.2 What procedures allow individuals to access their information?

7.3 Can individuals amend information about themselves in the system? If so, how?

7.4 Are there any privacy risks for this system that relate to individual participation? If so, how will GSA mitigate these risks?

SECTION 8.0 AWARENESS AND TRAINING

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

8.2 Are there any privacy risks for this system that relate to awareness and training? If so, how will GSA mitigate these risks?

SECTION 9.0 ACCOUNTABILITY AND AUDITING

9.1 How does the system ensure that the information is used in accordance with the stated practices in this PIA?

9.2 Are there any privacy risks for this system that relate to accountability and auditing? If so, how will GSA mitigate these risks?

Document purpose

This document contains important details about GSA Government Retirement Benefits (GRB) Information System. GSA IT must, in the course of calculating retirement benefits and tracking retirement cases, collect personally identifiable information (“PII”) about the people who use such products and services. PII is any information^[1] that can be used to distinguish or trace an individual’s identity like a name, address, or place and date of birth.

GSA uses Privacy Impact Assessments (PIAs) to explain how it collects, uses, secures, and destroys information in ways that protect privacy. This PIA is comprised of sections that reflect GSA’s [privacy policy](#) and [program goals](#). The sections also align to the Fair Information Practice Principles (“FIPPs”), a set of eight precepts that are codified in the Privacy Act of 1974.^[2]

System, Application or Project

Government Retirement Benefits (GRB) Information System

System, application or project includes information about

GSA Employees

System, application or project includes

- Name and other biographic information (e.g., date of birth)
- Contact Information (e.g., address, telephone number, email address)
- Social Security Number (SSN), Driver’s License Number or other government-issued identifiers

Overview

The GSA Government Retirement Benefits (GRB) is a web-based application used by the General Services Administration (GSA) as a tool for electronic automation of retirement related functions used by the OHRM. GSA’s GRB system resides within GSA’s IT operational environment that has a leasing agreement with GRB to use its application code and intellectual property. GSA HR users access the GRB application via the GSA Intranet and use the tool for calculating retirement benefits and tracking retirement cases.

PII is collected for the purpose of determining eligibility and applying for retirement at GSA.

System of Records Notices (SORNs) -

- [GSA/Agency-1](#), Employee Related Files, 61-FR-60103 November 26, 1996
- [OPM-GOVT-1](#), General Personnel Records, 77-FR-73694 December 11, 2012

SECTION 1.0 PURPOSE OF COLLECTION

GSA states its purpose and legal authority before collecting PII.

1.1 Why is GSA collecting the information?

The GSA Government Retirement Benefits (GRB) is a web-based application used by the General Services Administration (GSA) as a tool for electronic automation of employee retirement related functions used by the Office of Human Resource Management (OHRM). GSA's GRB system resides on premise in GSA operational data centers and has a leasing agreement with GRB for the use of the application system. GSA HR users access the GRB application via the Intranet and use the tool for calculating retirement benefits and tracking retirement applicant cases. Information stored and processed by GRB includes retirement information for the applicant and in some cases spouse and dependent information.

1.2 What legal authority and/or agreements allow GSA to collect the information?

Calculating retirement benefits and tracking retirement applicant cases requires collecting PII. In addition 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107 are the authorities for maintaining personnel information. Authorities for recording Social Security Numbers are E.O. 9397, 26 CFR 31.6011(b)-2, and 26 CFR 31.6109-1.

1.3 Is the information searchable by a personal identifier, for example a name or Social Security Number? If so, what System of Records Notice(s) apply/applies to the information being collected?

Yes, information is searchable by name or SSN. See the system of Records Notice (SORNs) that cover GRB for additional information -

- GSA/Agency-1, 61-FR-60103 November 26, 1996
- OPM-GOVT-1, 77-FR-73694 December 11, 2012

1.4. Has any information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)? If yes, provide the relevant names, OMB control numbers, and expiration dates.

No ICR has been submitted as this is not an information collection under the Paperwork Reduction Act (PRA).

1.5. Has a records retention schedule been approved by the National Archives and Records Administration (NARA)? Explain how long and for what reason the information is retained.

GRB complies with all GSA retention and disposal procedures specified by 1820.1 OAS P GSA Records Management Program. Records contained in the GRB system will be retained consistent with section 2.2 of NARA General Records Schedule, "Employee Management Records". See <https://www.archives.gov/files/records-mgmt/grs/trs29-sch-only.pdf>

Disposition Authority Number: DAA-GRS-2016-0014-0001 - Destroy when 3 years old, or 3 years after superseded or obsolete, whichever is appropriate, but longer retention is authorized if required for business use.

1.6. Are there any privacy risks that relate to the purpose of the collection? If so, how will GSA mitigate these risks?

There is a risk of the PII information becoming exposed if the system were to be compromised. The GRB system is only accessible from the internal GSA network. GSA has mitigated this risk through implementing FISMA Moderate 800.53 security controls.

SECTION 2.0 OPENNESS AND TRANSPARENCY

GSA is open and transparent. It notifies individuals of the PII it collects and how it protects, uses and shares it. It provides straightforward ways for individuals to learn about how GSA handles PII.

2.1 Will individuals be given notice prior to the collection and/or sharing of personal information about themselves? If not, please explain.

Yes, GSA employees are given prior notice when onboarding to GSA that their personnel information will be collected for employment administration.

2.2 Are there any privacy risks for this system that relate to openness and transparency? If so, how will GSA mitigate these risks?

No. GSA employees receive public notice of the information practices and the privacy impact of the programs from this PIA, the GSA and OPM SORNs and the eOPF and SF-50 documents. GRB has data entered into the system from the eOPF and SF-50.

SECTION 3.0 DATA MINIMIZATION

GSA limits the collection of PII to what is needed to accomplish the stated purpose for its collection. GSA keeps PII only as long as needed to fulfill that purpose.

3.1 Whose information is included in the system, application or project?

GSA Employees

3.2 What PII will the system, application or project include?

PII Collected shown below. All PII collected is for the purpose of applying for retirement at GSA.

- o Employee First, Middle Initial, Last Name
- o Employee SSN
- SSNs are generally the common element linking information among agencies, OPM, Shared Service Providers (human resources, payroll, and training), and benefit providers, some of which are legally required to use SSN.¹
 - o Employee date of birth (DoB)
 - o Employee Address
 - o Employee Phone
 - o Employee Email

The PII collected can be seen by GSA HR Specialists and HR Managers who review employee retirement cases.

3.3 Why is the collection and use of the PII necessary to the system, application or project?

¹ See Statement of OPM CIO David DeVries: "[Protecting Americans' Identities: Examining Efforts to Limit the Use of Social Security Numbers](#)" on May 23, 2019.

GRB is a web-based application used by GSA to electronically automate employee retirement related functions used by the Office of Human Resources Management (OHRM). GSA's GRB system resides on premise in GSA operational data centers and has a leasing agreement with GRB for the use of the application system. GSA HR users access the GRB application via the Intranet and use the tool for calculating retirement benefits and tracking retirement applicant cases.

Information stored and processed by GRB includes retirement information for the applicant and in some cases spouse and dependent information.

3.4 Will the system, application or project create or aggregate new data about the individual? If so, how will this data be maintained and used?

GRB does create or aggregate new data about the individual. The system calculates retirement benefits and dates.

3.5 What protections exist to protect the consolidated data and prevent unauthorized access?

GSA has implemented the required security and privacy controls according to NIST SP 800-53. GSA employs a variety of security measures designed to ensure that information is not inappropriately disclosed or released. These measures include security and privacy controls for access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.

3.6 Will the system monitor the public, GSA employees or contractors?

GRB does not monitor retirement applicants.

3.7 What kinds of report(s) can be produced on individuals?

GRB may create reports related to retirement applicants for determination of retirement benefits and eligibility.

3.8 Will the data included in any report(s) be de-identified? If so, what process(es) will be used to aggregate or de-identify the data?

GRB does not de-identify data for reporting. GSA uses the system to generate all OPM retirement applications and supporting forms and those forms require identifying information about GSA employees be included.

3.9 Are there any privacy risks for this system that relate to data minimization? If so, how will GSA mitigate these risks?

Given the reporting capability, the security and privacy measures include access controls, awareness and training for users and auditing capability to ensure accountability.

SECTION 4.0 LIMITS ON USES AND SHARING OF INFORMATION

GSA publishes a notice about how it plans to use and share any PII it collects. GSA only shares PII in ways that are compatible with the notice or as stated in the Privacy Act.

4.1 Is the information in the system, application or project limited to only the information that is needed to carry out the purpose of the collection?

The GRB system limits information to only what is required to carry out retirement activities.

GRB Inc. (vendor) may access applicant data when working to resolve reported system issues or to support GRB inquiries or run reports.

4.2 Will GSA share any of the information with other individuals, Federal and/or state agencies, or private sector organizations? If so, how will GSA share the information?

GSA will share GRB all of the PII listed in section 3.1 with OPM as federally mandated.

4.3 Is the information collected directly from the individual or is it taken from another source? If so, what is the other source(s)?

The information collected for GRB is manually entered from eOPF and SF-50 sources.

4.4 Will the system, application or project interact with other systems, applications or projects, either within or outside of GSA? If so, who, how and is a formal agreement(s) in place?

GRB is a standalone system with no electronic interaction with other systems.

4.5 Are there any privacy risks for this system, application or project that relate to use limitation? If so, how will GSA mitigate these risks?

Privacy Risk:

GSA collects sensitive Personally Identifiable Information (PII). Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional, and/or financial harm may result for the individuals affected.

Mitigation:

GSA has implemented the required security and privacy controls according to NIST SP 800-53. GSA employs a variety of security measures designed to ensure that information is not inappropriately disclosed or released. These measures include security and privacy controls for access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.

SECTION 5.0 DATA QUALITY AND INTEGRITY

GSA makes reasonable efforts to ensure that all PII it maintains is accurate, relevant, timely, and complete.

5.1 How will the information collected be verified for accuracy and completeness?

HR Specialists transcribe the info from the SF-50 and eOPF and then share that information with the retirement applicant to validate the accuracy of the information in GRB. The info is sent to the retiring employee usually by GSA email account and sometimes via certified U.S. mail, return receipt requested.

5.2 Are there any privacy risks for individuals whose information is collected or used that relate to data quality and integrity? If so, how will GSA mitigate these risks?

There is a risk of the PII information becoming exposed if the system were to be compromised. GSA retirement data is logged and audited and otherwise controlled to ensure integrity.

SECTION 6.0 SECURITY

GSA protects PII from loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

6.1 Who or what will have access to the data in the system, application or project? What is the authorization process to gain access?

The GRB system allows access to sensitive PII data on either an individual or administrative role basis. The access authorization is covered under the SP 800-53 access controls.

6.2 Has GSA completed a system security plan for the information system(s) or application?

A system security plan has been developed for GRB on August 1, 2019.

6.3 How will the system or application be secured from a physical, technological, and managerial perspective?

GSA has implemented the required security and privacy controls according to NIST SP 800-53. GSA employs a variety of security measures designed to ensure that information is not inappropriately disclosed or released. These measures include security and privacy controls for access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.

6.4 Are there mechanisms in place to identify suspected or confirmed security incidents and breaches of PII? If so, what are they?

GSA has implemented an Incident Response process that identifies breaches to PII through the implementation of the GSA Incident Response policy and procedure.

6.5 Are there any privacy risks for this system, application or project that relate to security? If so, how will GSA mitigate these risks?

Privacy Risk:

GRB collects sensitive PII. Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional, and/or financial harm may result for the individuals affected.

Mitigation:

GSA has implemented the required security and privacy controls according to NIST SP 800-53. GSA employs a variety of security measures designed to ensure that information is not inappropriately disclosed or released. These measures include security and privacy controls for access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.

SECTION 7.0 INDIVIDUAL PARTICIPATION

GSA provides individuals the ability to access their PII and to correct or amend it if it is inaccurate. If GSA exempts a system or program from access, amendment and other provisions of the Privacy Act, it notifies the public of that exemption.

7.1 What opportunities are available for individuals to consent to uses, decline to provide information or opt out of providing information? If no opportunities exist to consent, decline or opt out, please explain.

GSA employees consent to use of information upon employment with the Federal government. Each of the retirement eligibility forms (e.g. [SF-2801](#), “Application for Immediate Retirement” includes a Privacy Act Notice detailing the authorization of the collection of the sensitive information and the impact of not providing it).

7.2 What procedures allow individuals to access their information?

Individual can request reviews of their retirement calculations and eligibility through engagement with GSA’s OHRM.

GSA HR retirement Specialists and HR Managers gain access to GRB through GSA's Enterprise Access Request System (EARS) and the retirement information/changes would be processed through EARS.

EARS is used to provision, track, and audit GSA employee/contractor access to GSA applications. EARS works in conjunction with Rational ClearQuest for account approval, account management, and re-certification and has Authority to Operate under the Ancillary Financial Applications (AFA) FISMA Moderate boundary.

EARS ensures adherence to GSA Access Control policies ensuring personnel authorization best practices are implemented and followed when authorizing application access. The use of EARS systematically implements the general activities for authorizing personnel to access IT resources.

7.3 Can individuals amend information about themselves? If so, how?

Yes, GSA employees can request their information from OHRM and request changes from OHRM either via the forms they receive or they can request that the retirement specialists make the changes on their behalf.

7.4 Are there any privacy risks for this system, application or project that relate to individual participation? If so, how will GSA mitigate these risks?

Yes, individuals must take an active interest and participate in their retirement planning or else potential errors in retirement calculations and eligibility may not be addressed in a timely fashion.

SECTION 8.0 AWARENESS AND TRAINING

GSA trains its personnel to handle and protect PII properly.

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the system, application or project.

GSA is responsible for providing security awareness training to its employees and contractors who have a GSA network account. It is given as part of the on-boarding process to all GSA employees and contractors and these employees must have completed their security awareness training prior to gaining access to the GRB environment. In addition, GRB users must undergo and pass a minimum background investigation (MBI)

and complete role-based privacy awareness training prior to being granted access to GRB.

8.2 Are there any privacy risks for this system, application or project that relate to awareness and training? If so, how will GSA mitigate these risks?

No, GRB system users (GSA employees) are required to take security and privacy awareness and role-based training prior to being granted access to the system and annually thereafter.

SECTION 9.0 ACCOUNTABILITY AND AUDITING

GSA's Privacy Program is designed to make the agency accountable for complying with the Fair Information Practice Principles. GSA regularly checks that it is meeting the requirements and takes appropriate action if it is not.

9.1 How does the system, application or project ensure that the information is used in accordance with the stated practices in this PIA?

GSA personnel accessing the GRB system are required to adhere to the GSA Rules of Behavior.

9.2 Are there any privacy risks for this system, application or project that relate to accountability and auditing? If so, how will GSA mitigate these risks?

No privacy risks that relate to accountability and auditing due to GSA implementation of the required security and privacy controls according to NIST SP 800-53. The auditing of GRB is only for tracking users access, updates, and modifications to objects. No PII information is collected during the audit process.

^[1] OMB Memorandum [Preparing for and Responding to a Breach of Personally Identifiable Information](#) (OMB M-17-12) defines PII 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." The memorandum notes that "because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad."

^[2] Privacy Act of 1974, 5 U.S.C. § 552a, as amended.