Privacy Office Contact Information

Please send any questions by email to gsa.privacyact@gsa.gov or by U.S. Mail to:
General Services Administration
Chief Privacy Officer
1800 F Street NW
Washington, DC 20405

Document Purpose

This document contains important details about a GSA managed System, Application, or Project (identified below by the Authorization Package name). To accomplish its mission the GSA Office it supports must, in the course of business operations, 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, maintains, disseminates, uses, secures, and destroys information in ways that protect privacy. This PIA comprises 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 codified in the Privacy Act of 1974.[2]

[1]OMB Memorandum Preparing for and Responding to the 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.

General Information

PIA Identifier: 392
System Name: Government Retirement Benefits (GRB)
CPO Approval Date: 10/7/2022
PIA Expiration Date: 10/6/2025

Information System Security Manager (ISSM) Approval

Richard Banach

System Owner/Program Manager Approval

Monica Shackelford

Chief Privacy Officer (CPO) Approval

Richard Speidel

PIA Overview

A: System, Application, or Project Name:
Government Retirement Benefits (GRB)

B: System, application, or project includes information about:
GSA Employees

C: For the categories listed above, how many records are there for each?
approximately 61K employee records and 74 user records

D: System, application, or project includes these data elements:

- 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 PII Collected shown below. All PII collected is for the purpose of applying for retirement at GSA.
- Employee First, Middle Initial, Last Name
- 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.
- Employee date of birth (DoB) o Employee Address
- Employee Phone
- Employee Email

The data elements on spouse only (no children information is kept) are listed as follows: SSN Full Name (Prefix, First Name, Middle Initial, Last Name, Suffix) Date of Birth Gender Date of Marriage Place of Marriage The PII collected can be seen by GSA HR Specialists and HR Managers who review employee retirement cases.

Overview:

1.0 Purpose of Collection

1.1: What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
The authorities for collecting the information are 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107 are. Authorities for recording Social Security Numbers are E.O. 9397, 26 CFR 31.6011(b)2, and 26 CFR 31.61091.

1.2: Is the information searchable by a personal identifier, for example a name or Social Security number?
Yes

1.2a: If so, what Privacy Act System of Records Notice(s) (SORN(s) applies to the information being collected?
Existing SORN applicable

1.2: System of Records Notice(s) (Legacy Text): What System of Records Notice(s) apply/applies to the information?
GSA/Agency-1, 61-FR-60103 November 26, 1996 OPM-GOVT-1, 77-FR-73694 December 11, 2012

1.2b: Explain why a SORN is not required.

1.3: Has an information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)?

1.3: Information Collection Request: Provide the relevant names, OMB control numbers, and expiration dates.

1.4: What is the records retention schedule for the information systems(s)? Explain how long and for what reason the information is kept.
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.

2.0 Openness and Transparency

2.1: Will individuals be given notice before the collection, maintenance, use or dissemination and/or sharing of personal information about them? Yes

2.1 Explain: If not, please explain.

3.0 Data Minimization

3.1: Why is the collection and use of the PII necessary to the project or system?
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 licensing agreement with GRB Inc. (vendor) 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.

3.2: Will the system, application, or project create or aggregate new data about the individual?
Yes

3.2 Explained: 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.

3.3 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.

3.4 Will the system monitor the public, GSA employees, or contractors?
None

3.4 Explain: Please elaborate as needed.
GRB does not monitor retirement applicants.

3.5 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.

3.6 Will the data included in any report(s) be de-identified?
No

3.6 Explain: If so, what process(es) will be used to aggregate or de-identify the data?

3.6 Why Not: Why will the data not be de-identified?
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 that identifying information about GSA employees be included.

4.0 Limits on Using and Sharing 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?
Yes

4.2: Will GSA share any of the information with other individuals, federal and/or state agencies, or private-sector organizations?

Federal Agencies

4.2How: If so, how will GSA share the information?
GSA will share the PII listed in section 3.1 with OPM as federally mandated.

4.3: Is the information collected:
From Another Source

4.3Other Source: 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?
No

4.4WhoHow: If so, who and how?

4.4Formal Agreement: Is a formal agreement(s) in place?
No

4.4NoAgreement: Why is there not a formal agreement in place?
GRB is a standalone system with no electronic interaction with other systems. Information from GRB is manually rekeyed into other systems such as HRLinks.

5.0 Data Quality and Integrity

5.1: How will the information collected, maintained, used, or disseminated 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.

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?
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.

6.1b: What is the authorization process to gain access?
The access authorization is covered under the SP 800-53 access controls.

6.2: Has a System Security Plan (SSP) been completed for the Information System(s) supporting the project?
Yes

6.2a: Enter the actual or expected ATO date from the associated authorization package.
10/1/2022

6.3: How will the system or application be secured from a physical, technical, 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 and respond to suspected or confirmed security incidents and breaches of PII?
Yes

6.4What: 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.

7.0 Individual Participation

7.1: What opportunities do individuals have to consent or decline to provide information?
GSA employees consent to use of information upon employment with the Federal government. Each of the retirement eligibility forms (e.g. , "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).

7.1Opt: Can they opt-in or opt-out?
No

7.1Explain: If there are no opportunities to consent, decline, opt in, 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 are the procedures that allow individuals to access their information?
Individuals do not access their information in GRB. They 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?
No

7.3How: How do individuals amend information about themselves?

8.0 Awareness and Training

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 annual security and privacy 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.

9.0 Accountability and Auditing

9.1: How does the system owner ensure that the information is used only according to the stated practices in this PIA?
GSA personnel accessing the GRB system are required to adhere to the GSA Rules of Behavior.