

**U.S. Department of Commerce
U.S. Census Bureau**



**Privacy Impact Assessment
for the
Office of the Chief Administrative Office (OCAO) Government
Retirement Benefits (GRB) System**

Reviewed by: Donna Neal, Bureau Chief Privacy Officer

- ☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Donna Neal

Digitally signed by Donna Neal 11/26/24
Date: 2024.11.26 09:36:37 -05'00'

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Date

**U.S. Department of Commerce Privacy Impact Assessment
U.S. Census Bureau/ Office of the Chief Administrative Office
(OCAO) Government Retirement Benefits (GRB) System**

Unique Project Identifier: 006-000401700

Introduction: System Description

Provide a brief description of the information system.

The GRB system is a Software as a Service for retirements benefits management and planning. It is updated with sensitive federal employee data from the Department of Agriculture's National Finance Center (Federal payroll center). The cloud-based contactor-managed system allows federal employees to track and manage their own retirement benefits. Within the GRB online system, customer responsible security controls and data updates will be managed by HRD Benefits Management personnel, while "single sign-on" capability for the Census Federal employees will be managed by the Census Bureau's Telecommunications office, which is falls under the OCIO Data Communications boundary.

Address the following elements:

(a) Whether it is a general support system, major application, or other type of system

GRB is a minor application provided by the vendor's software as a service (SaaS) cloud offering.

(b) System location

The GRB system is hosted by GRB Inc in their cloud environment. GRB Inc's headquarters location is Alexandria, VA.

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

Census use of GRB has no interconnections to other systems.

(d) The way the system operates to achieve the purpose(s) identified in Section 4

GRB is a web-based application that provides inference calculation of federal government employee retirement and other benefits per the latest applicable laws governing Civil Service

Retirement System (CSRS) and Federal Employees Retirement System (FERS) retirement programs. Additionally, the application generates approved versions of forms required for processing that meet standards and guidance set forth by the Office of Personnel Management (OPM). The service shall be accessible to users 24/7.

(e) How information in the system is retrieved by the user

Currently employed Federal Employees and HR benefits management specialists will authenticate to GRB using their federal (Census) email address as the primary authenticator for logon and data retrieval. After separation from federal employment employees will no longer have access to the GRB system.

(f) How information is transmitted to and from the system

The Census Bureau Human Resources Division (HRD) will compile four reports from the National Finance Center (NFC), managed by the United States Department of Agriculture (USDA), manually uploaded via secure file transfer protocol (SFTP).

Employee and HRD web access uses HTTPS encrypted web services.

(g) Any information sharing

Data entered into the GRB system for Census employee retirements benefits analysis will not be shared outside of the GRB system.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

5 U.S.C. Chapters 83 & 84 and Section 301
E.O. 9397, as amended by 13478
44 U.S.C. Section 3101
44 U.S.C. Section 3309
44 U.S.C. Chapter 33

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

Moderate

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.

_____ This is an existing information system with changes that create new privacy risks.
(Check all that apply.)

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

_____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

 X This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. (Check all that apply.)

Identifying Numbers (IN)					
a. Social Security*	X	f. Driver's License		j. Financial Account	
b. Taxpayer ID		g. Passport		k. Financial Transaction	
c. Employer ID		h. Alien Registration		l. Vehicle Identifier	
d. Employee ID		i. Credit Card		m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify): user id also known as James bond id (Jbid)					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form: National Finance records from which the retirements benefits data for an employee are tracked is organized under SSN for unique identification.					

General Personal Data (GPD)					
a. Name	X	h. Date of Birth	X	o. Financial Information	X
b. Maiden Name	X	i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address	X	q. Military Service	X
d. Gender	X	k. Telephone Number	X	r. Criminal Record	
e. Age	X	l. Email Address		s. Marital Status	X
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			

u. Other general personal data (specify):

Work-Related Data (WRD)					
a. Occupation		e. Work Email Address	X	i. Business Associates	
b. Job Title	X	f. Salary	X	j. Proprietary or Business Information	
c. Work Address	X	g. Work History	X	k. Procurement/contracting records	
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information			
l. Other work-related data (specify): Retirement benefits data					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording		i. Height		n. Retina/Iris Scans	
e. Photographs		j. Weight		o. Dental Profile	
p. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address		f. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person		Hard Copy: Mail/Fax		Online	
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	X
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

The uploaded HRD data to GRB originates from NFC's Payroll/Personnel System (PPS) which maintains employee personnel records and time and attendance data for federal employees. Individuals are able to view their own personal information however they are not able to update any information within GRB; individuals may contact their servicing HR office to update information.
--

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. 1545-0074, 3206-0032, 3206-0042, 3206-0099, 3206-0190, 3206-0234, 3206-0156, 3206-0128, 3206-0134, 3206-0160, 3206-0230, 3206-0136, 3206-0173, 3206-0172, 3206-0170, 3206-0134, 3206-0228, 3206-0275
	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.
---	--

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities

Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X	There are not any IT system supported activities which raise privacy risks/concerns.
---	--

Section 4: Purpose of the System

- 4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated.
(Check all that apply.)

Purpose			
For a Computer Matching Program		For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

- 5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

<u>For Administrative Matters and Administering Human Resources Programs:</u> Within GRB, all PII is transferred from official sources (National Finance Center via SFTP transfer/ Official OPM and Census HRD managed personnel records are manually entered; however, this will be phased out when the system becomes fully operational.) This PII is used for retirements benefits management and planning.
--

- 5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

The U.S. Census Bureau use of data/information presents possible threats such as internal breaches caused by employees within an organization. Today's most damaging security threats are not originating from malicious outsiders or malware but from trusted insiders - both malicious insiders and negligent insiders. Inside threats are not just malicious employees that intend to directly harm the Bureau through theft or sabotage. Negligent employees can unintentionally cause security breaches and leaks by accident. To prevent or mitigate potential threats to privacy the U.S. Census Bureau has put into place mandatory training for all system users. All Census Bureau employees and contractors undergo mandatory annual data stewardship training to include proper handling, dissemination, and disposal of BII/PII/Title 13/Title 26 data.

In addition, the Census Bureau Information technology systems employ a multitude of layered security controls to protect PII/BII at rest, during processing, as well as in transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level, including, but not limited to the following:

- Intrusion Detection | Prevention Systems (IDS | IPS)
- Firewalls
- Mandatory use of HTTP(S) for Census Bureau Public facing websites
- Use of trusted internet connection (TIC)
- Anti-Virus software to protect host/end user systems
- Encryption of databases (Data at rest)
- HSPD-12 Compliant PIV cards
- Access Controls
- SFTP Encryption during NFC data transfer

The Census Bureau Information technology systems also follow the National Institute of Standards and Technology (NIST) standards including special publications 800-53, 800-63, 800-37 etc. Any system within the Census Bureau that contains, transmits, or processes BII/PII has a current authority to operate (ATO) and goes through continuous monitoring on a yearly basis to ensure controls are implemented and operating as intended. The census Bureau also deploys a Data Loss Prevention solution.

The information in GRB is handled, retained and disposed of in accordance with appropriate federal record schedules.

GRB is an OPM registered FedRAMP authorized Software as a Service (SaaS) rated MODERATE and subject to ongoing authorization and continuous monitoring of security controls to validate security compliance.

Section 6: Information Sharing and Access

- 6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau			
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

X	The PII/BII in the system will not be shared.
---	---

- 6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
X	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

- 6.3 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: There are no system interconnections. GRB receives PII from the NFC via a SFTP transfer initiated by authorized Census Bureau Human Resources Division (HRD) employees. HRD will compile four reports from the National Finance Center (NFC) and securely transfer them to the GRB platform on a bi-weekly basis using the Bureaus enterprise managed and validated SFTP tool.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

- 6.4 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://www.census.gov/about/policies/privacy/privacy-policy.html	
X	Yes, notice is provided by other means.	Specify how: GRB provides a notice upon logging on to the web application. In addition, PII within GRB is not collected directly from individuals, it is received from OPM and the National Finance Center. This information is mandatory under the terms of Federal employment. A Privacy Act statement is provided to individual(s) at the time the information is collected.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: PII within GRB is not collected directly from individuals, it is received from OPM and the National Finance Center. This information is mandatory under the terms of Federal employment, so individuals do not have an opportunity to decline to provide PII/BII.

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: PII within GRB is not collected directly from individuals, it is received from OPM and the National Finance Center. This information is mandatory under the terms of Federal employment, so individuals do not have an opportunity to consent to particular uses of their PII/BII.

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Individuals are able to review but not update information within the appropriate Census Bureau applications. In addition, individuals may contact their servicing HR office to update information (GRB).
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

X	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Only authorized government/contractor personnel are allowed to access PII/BII within a system. Authorizations for users occur yearly, at a minimum in accordance with applicable Bureau, Agency, and Federal policies/guidelines. In addition, audit logs are in place and assessed per NIST control AU-03, Content of Audit records.
X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 1/26/2024 This is a new system. The A&A date will be provided when the A&A package is approved
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish DOC ownership rights over data including PII/BII.

	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

- 8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.
(Include data encryption in transit and/or at rest, if applicable).

Census Bureau Information technology systems employ a multitude of layered security controls to protect BII/PII at rest, during processing, as well as in transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level including, but not limited to the following: • Intrusion Detection Prevention Systems (IDS IPS) • Firewalls • Mandatory use of HTTP(S) for Census Public facing websites • Use of trusted internet connection (TIC) • Anti-Virus software to protect host/end user systems • Encryption of transferred files via SFTP • Encryption of databases (Data at rest) • HSPD-12 Compliant PIV cards • Access Controls Census Bureau Information technology systems also follow the National Institute of Standards and Technology (NIST) standards including special publications 800-53, 800-63, 800-37 etc. Any system within the Census Bureau that contains, transmits, or processes BII/PII has a current authority to operate (ATO) and goes through continuous monitoring on a yearly basis to ensure controls are implemented and operating as intended. The Census Bureau also deploys a Data Loss Prevention (DLP) solution/tool as well.
--

Section 9: Privacy Act

- 9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

 X Yes, the PII/BII is searchable by a personal identifier.

 No, the PII/BII is not searchable by a personal identifier.

- 9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (A new system of records notice (SORN) is required if the system is not covered by an existing SORN).

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. (list all that apply): COMMERCE/DEPT-1: Attendance, Leave, and Payroll Records of Employees and Certain Other Persons, http://www.osec.doc.gov/opog/PrivacyAct/SORNS/dept-1.html OPM GOVT -1:General Personnel Records, https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-1-general-personnel-records.pdf
---	---

	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: GRS 2.4-Employee Compensation and Benefits Records, GRS 3.1-General Technology Management Records, GRS 3.2-Information Systems Security Records
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	X
Degaussing	X	Deleting	X
Other (specify): GRB under the FedRAMP SaaS shared-responsibility model manages the deletion, shredding and degaussing methods for data and media disposition under their scope of control and responsibilities.			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. (both)
X	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact level.
(Check all that apply.)

X	Identifiability	Provide explanation: Combined data elements uniquely and directly identify individuals.
X	Quantity of PII	Provide explanation: A serious or substantial number of individuals affected by loss, theft, or compromise. Serious collective harm to individuals, harm to the organization's reputation, or cost to the organization in addressing a breach.
X	Data Field Sensitivity	Provide explanation: Data fields, alone or in combination, may be relevant in some other contexts and may, in those contexts, make the individual or organization vulnerable to harms, such as identity theft, embarrassment, loss of trust, or costs.
X	Context of Use	Provide explanation: Disclosure of the act of collecting, and using the PII, or the PII itself may result in serious harm to the individual or organization.
X	Obligation to Protect Confidentiality	Provide explanation: Role-specific privacy laws, regulations or mandates (e.g., those that cover certain types of healthcare or financial information) apply that add more restrictive requirements to government-wide requirements. Violations may result in serious civil or criminal penalties.
X	Access to and Location of PII	Provide explanation: Located on computers and other devices on a network not controlled by the organization. Access limited to a small population of the organization's workforce, such as a program or office which owns the information on behalf of the organization.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data,

include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

Although this IT system can only be accessed by authorized individuals that have a business need to know, the potential risk from insider threat to the organization, which may cause harm such as identity theft, embarrassment, loss of trust, or cost, still exists. The Census Bureau conducts routine security awareness training on recognizing and reporting potential indicators of insider threat. Insider threat is always possible. In addition to the security protocols already described in this assessment, the Census Bureau limits access to sensitive information to sworn employees who have an authorized business need to know.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

X	Yes, the conduct of this PIA results in required technology changes. Explanation: While the adoption of the GRB FedRAMP SaaS technology capabilities is the driver for this PIA analysis, some of the retirement benefits management and planning workflows that are manually performed by OCAO Human Resources Division may be subject to requirements in line with the technology changes.
	No, the conduct of this PIA does not result in any required technology changes.