



Privacy Impact Assessment for the VA IT System called:

Government Retirement and Benefits (GRB) Platform – Enterprise Human Resources Operations Office (HROO)

Date PIA submitted for review:

May 9, 2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Kimberly Murphy	Kimberly.Murphy@va.gov	781-331-3206
Information System Security Officer (ISSO)	Hurst McGraff	McGraff.Hurst@va.gov	512-326-6438
Information System Owner	Chino Walters	Chino.Walters@va.gov	202-461-0452

Abstract

Government Retirements and Benefits (GRB) Full Platform is a web-based system that allows Federal Employees and Federal Retirements and Benefits Specialists to access the system with a web browser client via the Internet. GRB Full Platform provides benefits specialist tools to perform their day-to-day job (i.e., preparing service histories, creating retirement estimate reports, as well as various other related estimate reports).

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

1 General Description

- A. *The IT system name and the name of the program office that owns the IT system.*

IT System Name: Government Retirement and Benefits (GRB) Platform – Enterprise

Name of the program office: Human Resources Operations Office (HROO, Veteran’s Health Administration (VHA)

- B. *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*

The Retirement Shared Service Office, Workforce Management and Consulting will be operating the Government Retirements and Benefits (GRB) Full Platform owned by Government Retirements and Benefits Inc. GRB is a web-based application that assists in calculating an employee’s retirement options and benefits. Transitioning to GRB Full Platform will provide consistency across the VA agency. This will encompass approximately 410,000 employee records. GRB includes functionality for HR Specialists and for use via self-service.

- C. *Indicate the ownership or control of the IT system or project.*

VA Controlled, none-VA owned and operated

2. Information Collection and Sharing

- D. *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*

All VHA employees approximately 44, 000

- E. *A general description of the information in the IT system and the purpose for collecting this information.*

GRB requires the use of PII, which will be provided to GRB through the Defense Finance and Accounting Service (DFAS) payroll system and HR Smart. DFAS serves as the data collection for the employment and compensation data used in GRB. HR Smart is the system of record for all employee data. Only pertinent PII that is necessary to accurately compute retirement estimates would be extracted from DFAS, including names, dates of birth, and Social Security numbers

Version Date: October 1, 2022

Page 2 of 33

(SSNs). In cases where there are gaps in the DFAS data provided (i.e., federal service from another agency, Retirement Shared Service Office's (RSSO) HR Specialists may manually input data from the user's federal employment history to complete the calculations.

- F. *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*

GRB receives information from DFAS using below steps: 1. Data set is manually queried from the DFAS system. 2. The .csv file is downloaded, encrypted with FIPS 140.2 or better, and saved onto the user's network drive. 3. The encrypted .csv file is sent securely via SFTP and uploaded into GRB. 4. The encrypted .csv file is permanently deleted from the user's network drive after a successful SFTP.

- G. *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*

N/A system only operate at one site

3. Legal Authority and SORN

- H. *A citation of the legal authority to operate the IT system.*

The legal authority to operate the system is 5 USC Titles 8415, 8339, 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.

SORN 27VA047; Personnel and Accounting Integrated Data System-VA;

<https://www.govinfo.gov/content/pkg/FR-2012-07-02/pdf/2012-16167.pdf>

- I. *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

N/A system is not in the process of being modified

D. System Changes

- J. *Whether the completion of this PIA will result in circumstances that require changes to business processes*

N/A no system changes required

- K. *Whether the completion of this PIA could potentially result in technology changes*

N/A no technology changes required

Section 1. Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

1.1 What information is collected, used, disseminated, created, or maintained in the system?

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (II), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (<https://vavww.va.gov/vapubs/>). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.

This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional SPI is collected, used, disseminated, created, or maintained, please list those in the text box below:

- | | | |
|--|---|---|
| <input checked="" type="checkbox"/> Name | <input checked="" type="checkbox"/> Financial Information | <input checked="" type="checkbox"/> Gender |
| <input checked="" type="checkbox"/> Social Security Number | <input type="checkbox"/> Health Insurance | <input type="checkbox"/> Integrated Control |
| <input checked="" type="checkbox"/> Date of Birth | Beneficiary Numbers | Number (ICN) |
| <input type="checkbox"/> Mother's Maiden Name | Account numbers | <input type="checkbox"/> Military History/Service |
| <input checked="" type="checkbox"/> Personal Mailing | <input checked="" type="checkbox"/> Certificate/License | Connection |
| Address | numbers* | <input type="checkbox"/> Next of Kin |
| <input checked="" type="checkbox"/> Personal Phone | <input type="checkbox"/> Vehicle License Plate | <input checked="" type="checkbox"/> Other Data Elements |
| Number(s) | Number | (list below) |
| <input type="checkbox"/> Personal Fax Number | <input type="checkbox"/> Internet Protocol (IP) | |
| <input checked="" type="checkbox"/> Personal Email Address | Address Numbers | |
| <input type="checkbox"/> Emergency Contact | <input type="checkbox"/> Medications | |
| Information (Name, Phone | <input type="checkbox"/> Medical Records | |
| Number, etc. of a different | <input type="checkbox"/> Race/Ethnicity | |
| individual) | <input type="checkbox"/> Tax Identification | |
| | Number | |
| | <input type="checkbox"/> Medical Record | |
| | Number | |

Other Elements:

Version Date: October 1, 2022

Page 4 of 33

Spouse Date of Birth,
Dates of federal service,
Salary

Non-Sensitive
Information: Number of
Children, Gender,
Alternate Phone,
Address, City, State, Zip
code, Zip Plus Four,
County, Country, Other
Email, Married, Spouse
Social Security Number,
Spouse Name, Spouse
Gender, Date of
Marriage, Place of
Marriage, Current
Appointment Date,
Current Agency,
Retirement Code,
Annual Leave Balance,
Sick Leave Balance,
Frozen Sick Leave
Balance, FEGLI Code,
FEHB Code, Pay Basis,
Pay Rate, Excess
LWOP, Position
Description, CSRS
Special Service Abroad
Years, CSRS Special
Service Abroad Months,
FERS Special Service
Abroad Years, FERS
Special Service Abroad
Months, Unhealthful
Service Years,
Unhealthful Service
Months, Unhealthful
Service Days, Non-
Federal Credit Leave
Yrs, Non-Federal Credit
Leave Months, Pay
Plan, Grade, FEGLI
Base Check, FEGLI
Base, Country Code,
Position Title, Entered
on Duty Date, Annuitant
Indicator, Organization
Component, Personnel

Office Identifier, Frozen
CSRS Years, Frozen
CSRS Months, Frozen
CSRS Days, Frozen
LFA CSRS Years,
Frozen LFA CSRS
Months, Frozen LFA
CSRS Days, TSP
Contribution Amount,
TSP Agency
Contribution Amount,
TSP Contribution
Percentage, TSP Roth,
Contribution Amount,
TSP Roth, Contribution
Percentage, TSP
Traditional Deduction
Amount, TSP Roth
Deduction Amount,
From Record Data As
Of Date, From Record
SCD Congressional,
From Record SCD
Leave, From Record
SCD Retirement, From
Record Is Transferee,
From Record Military
Service Years, From
Record Military Service
Months, From Record
Military Service Days,
From Record Long
Term Care Insurance
Premium Monthly,
From Record SCD Law
Fire ATC, TSP Catchup
Contribution Amount,
TSP Contribution
Status, TSP Roth
Catchup Contribution
Amount, TSP Status
Date, TSP Reelect
Eligibility Date, FEHB
Regular Eligibility
Expiration Date, FEHB
In Premium Conversion
Plan Flag, FEHB
Required To Provide
Coverage To Dependent

End Date, FEHB In
Premium Conversion
Plan Flag, FEHB
Required To Provide
Coverage To Dependent
End Date, FEGLI
Eligibility Due To
Providing Medical Info
Expire Date, FEGLI
Eligibility Due
Reinstatement Due To
Break Expire Date,
FEGLI Eligibility Due
Reinstatement Due To
Break Excluded Expire
Date, FEGLI Eligibility
Due DoD And Civilian
Employees Affected By
Pub Law 106398 And
110417 Expire Date,
FEGLI Eligibility Due
DoD And Civilian
Employees Affected By
Pub Law 106398 And
110417 Expire Date
Included, Bank Name,
Bank Account Number,
Bank Routing Number,
Federal Withholding,
HCFSA Allotment
Monthly, DCFSA
Allotment Monthly, Lex
HCFSA Allotment
Monthly, FEDVIP
Dental Premium
Monthly, FEDVIP
Vision Premium
Monthly, FEGLI Option
Eligibility Expiration
Date, OPM Work
Schedule, Agency
Organization Name,
Agency Address,
Agency City, Agency
State, Agency Zip,
Agency Country,
Personnel Office
Contact Name,
Personnel Office Phone,

Payroll Office Number,
 Payroll Office Contact
 Name, Payroll Office
 Phone, Is Educator,
 Educator Leave Balance

Days, Payroll Provider,
 Servicing Personnel
 Office, From Date, To
 Date, Biweekly Tod,
 Pay Basis, Pay Rate,

Pay Rate, Year,
 Earnings

PII Mapping of Components (Servers/Database)

GRB consists of two key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by GRB and the reasons for the collection of the PII are in the table below.

Note: Due to the PIA being a public facing document, please do not include the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/Storage of PII	Safeguards
GRBDB1	Yes	Yes	Name, Social Security Number, Date of Birth, Personal Phone number, Personal Email address, Personal mailing address, Gender, Financial Information, Certificate/License numbers, Spouse Date of Birth, Dates of federal service, Salary, Other data elements listed in section 1.1.	GRB is a comprehensive commercial retirement benefits calculator platform that is web-based with capabilities to accurately compute various complex estimates needed in assisting employees with their retirement decisions. The calculator software is used for computing benefits and counseling employees under the Civil Service Retirement System (CSRS), Federal Employees Retirement System (FERS), the Federal Thrift Savings Plan and the Social	FIPS 140.2 Encryption

				Security program. Additionally, the application generates FIPS 140.2 Encryption Page 6 of 29 approved versions of form required for processing that meet standards and guidance set forth by the Office of Personnel Management (OPM). GRB will be receiving information from HR Smart and Defense Finance and Accounting System (DFAS).	
GRBDB2	Yes	Yes	Name, Social Security Number, Date of Birth, Personal Phone number, Personal Email address, Personal mailing address, Gender, Financial Information, Certificate/License numbers, Spouse Date of Birth, Dates of federal service, Salary, Other data elements listed in section 1.1.	GRB is a comprehensive commercial retirement benefits calculator platform that is web - based with capabilities to accurately compute various complex estimates needed in assisting employees with their retirement decisions. The calculator software is used for computing benefits and counseling employees under the Civil Service Retirement System (CSRS), Federal Employees Retirement System (FERS), the Federal Thrift FIPS 140.2 Encryption Page 7 of 29 Savings Plan and the Social Security program. Additionally, the application generates approved	FIPS 140.2 Encryption

				versions of form required for processing that meet standards and guidance set forth by the Office of Personnel Management (OPM). GRB will be receiving information from HR Smart and Defense Finance and Accounting System (DFAS).	
--	--	--	--	--	--

1.2 What are the sources of the information in the system?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

GRB does not collect PII from individuals. Information is be provided to GRB through the Defense Finance and Accounting Service (DFAS) payroll system and HR Smart.

1.2b Describe why information from sources other than the individual is required. For example, if a program’s system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

Information is gathered from the DFAS only when employee initiates a request, in order to process employee’s request.

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

N/A system does not create information

1.3 How is the information collected?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from

another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

GRB does not collect PII from individuals. Information is provided to GRB through the Defense Finance and Accounting Service (DFAS) payroll system and HR Smart.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.

N/A system does not collect information

1.4 How will the information be checked for accuracy? How often will it be checked?

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

HR Specialists review HR Smart, DFAS, and electronic Official Personnel File (eOPF) data for accuracy, 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 VA email account and sometimes via certified U.S. mail, Page 9 of 29 return receipt requested. Employees will have limited access to view some data in GRB to verify accuracy. The data will be checked at point of request for retirement services, and then checked again and validated by an employee through their employee signature(s) on various retirement forms.

1.4b If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

N/A system does not perform commercial aggregation

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect

The legal authorities are 5 USC Titles 8415, 8339, 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. SORN 27VA047; Personnel and Accounting Integrated DataSystem-VA; <https://www.govinfo.gov/content/pkg/FR-2012-07-02/pdf/2012-16167.pdf>

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete this section)

Consider the following Fair Information Practice Principles (FIPPs) when assessing the risk to individual privacy:

Principle of Purpose Specification: Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.

Principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program?

Principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual?

*Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?
This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.*

Follow the format below when entering your risk assessment:

Privacy Risk: Disclosure of personally identifiable information, that if disclosed may expose the respondent/subject to financial loss or identity theft.

Privacy Risk: Disclosure of military service details that may compromise the individual's reputation, circumstances, or safety.

Privacy Risk: Disclosure of medical, personal, or other information that may compromise the individual's reputation, circumstances, or safety. Page 10 of 29

Privacy Risk: Disclosure of participation in a study or activity, where knowledge of participation may adversely impact the individual's reputation or circumstances.

Mitigation: Information will be secured on the system through access controls, personnel security awareness and training, regular auditing of information and information management processes, careful monitoring of a properly authorized information system, control of changes to the system, appropriate

handling and testing of contingencies and contingency planning, ensuring that all users of the information system are properly identified and authorized for access, and that they are aware of the rules and acknowledge that fact, by ensuring that any incident is handled expeditiously, properly maintaining the system and regulating the environment the system operates in, controlling media, evaluating risks and planning for information management and information system operations, by ensuring that the system and any exchange of information is protected, by maintaining the integrity of the system and the information stored in it, and by adhering to the requirements established in applicable contracts.

Section 2. Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe how the information in the system will be used in support of the program's business purpose.

Identify and list each use (both internal and external to VA) of the information collected or maintained. This question is related to privacy control AP-2, Purpose Specification.

The system is designed to estimate retirement annuities for Federal employees. The application computes data associated with retirements such as annuities, survivor benefits, deposits/redeposits, etc. Information collected is used in following manner –

Name: Used as an identifier

SSN: Used as an identifier

Date of Birth: Used as an identifier

Phone #: Used to contact individual

Personal Mailing Address: To send employee their information

Personal Email Address: To send employee their information

Spousal Information (Name, DOB, SSN, Gender, Address, Email Address, Phone Number): For Beneficiary Information

2.2 What types of tools are used to analyze data and what type of data may be produced?

These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.

N/A system does not perform data analysis.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the

Version Date: October 1, 2022

individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

N/A system does not create new records

2.3 How is the information in the system secured?

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

2.3a What measures are in place to protect data in transit and at rest?

GRB Platform implements FIPS validated cryptography for data at rest and data in transit, externally and internally as follows:

Data in transit -

- Web server transmissions use TLS 1.2 Microsoft Cryptographic Primitives Library FIPS Cert#3544
- SFTP SSH 2.0 Microsoft Cryptographic Primitives Library FIPS Cert#3544
- Web Servers transmitting to database servers use application layer encryption Microsoft Cryptographic Primitives Library FIPS Cert#3544,
- SFTP servers to database servers use application layer encryption Microsoft Cryptographic Primitives Library FIPS Cert#3544.
- Database server backups to backup server use application layer encryption Microsoft Cryptographic Primitives Library FIPS Cert#3544.
- Email notifications: Sent from the system use TLS 1.2 Microsoft Cryptographic Primitives Library FIPS Cert#3544
- Update Sources – Updates pulled from update sources use TLS 1.2 Microsoft Cryptographic Primitives Library FIPS Cert#3544
- CSP Access – VPN connections use TLS 1.2 Cisco FIPS Object Module FIPS Cert #4174
- Log/Security Traffic – communications to logging aggregator use TLS 1.2 Microsoft Cryptographic Primitives Library FIPS Cert#3544
- CSP Updates – Updates from GRB use SSH 1.2 Microsoft Cryptographic Primitives Library FIPS Cert#3544

Data at rest –

- Data in database - use application layer encryption Microsoft Cryptographic Primitives Library FIPS Cert#3544
- Backups – use full disk encryption provided by Microsoft Bitlocker FIPS Certificate(s): #3502, #3501, #3092
- SFTP File - use full disk encryption provided by Microsoft Bitlocker FIPS Certificate(s): #3502, #3501, #3092

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?

All the above safeguards are implemented due to processing and retaining of Social Security Numbers

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?

GRB-e is hosted in the FedRAMP High/Moderate rated private Cloud. GRB (SaaS provider) maintains a FedRAMP ATO and a VA F-package within eMASS that outlines all OMB Memorandum M-06-15 safeguards and security mechanisms.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

*Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. **Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.***

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Is the PIA and SORN, if applicable, clear about the uses of the information?

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?

This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

2.4a How is access to the PII determined?

HR specialists are assigned cases by the HR manager. Only HR specialists and HR managers have access to PII.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented?

This is documented in GRB-e Access Control Standard Operating Procedure (SOP)

2.4c Does access require manager approval?

Yes - access is governed by HRPAS import which enables their customer access to GRB. Next, Supervisors notify GRB Admins to enable permissions for HR roles.

2.4d Is access to the PII being monitored, tracked, or recorded?

No. Only HR specialists and HR managers have access to PII.

2.4e Who is responsible for assuring safeguards for the PII?

PII safeguarding is one of the key responsibilities for all HR personnel.

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

*Identify and list all information collected from question 1.1 that is **retained** by the system.*

This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal

Name, Social Security Number, Date of Birth, personal email address, personal phone number, personal email address, certificate/license numbers, Spouse Date of Birth, Dates of federal service, Salary, Number of Children, Gender, Alternate Phone, Address, City, State, Zip code, Zip Plus Four, County, Country, Other Email, Married, Spouse Social Security Number, Spouse Name, Spouse Gender, Date of Marriage, Place of Marriage, Current Appointment Date, Current Agency, Retirement Code, Annual Leave Balance, Sick Leave Balance, Frozen Sick Leave Balance, FEGLI Code, FEHB Code, Pay Basis, Pay Rate, Excess LWOP, Position Description, CSRS Special Service Abroad Years, CSRS Special Service Abroad Months, FERS Special Service Abroad Years, FERS Special Service Abroad Months, Unhealthful Service Years, Unhealthful Service Months, Unhealthful Service Days, Non-Federal Credit Leave Yrs, Non-Federal Credit Leave Months, Pay Plan, Grade, FEGLI Base Check, FEGLI Base, Country Code, Position Title, Entered on Duty Date, Annuitant Indicator, Organization Component, Personnel Office Identifier, Frozen CSRS Years, Frozen CSRS Months, Frozen CSRS Days, Frozen LFA CSRS Years, Frozen LFA CSRS Months, Frozen LFA CSRS Days, TSP Contribution Amount, TSP Agency Contribution Amount, TSP Contribution Percentage, TSP Roth, Contribution Amount, TSP Roth, Contribution Percentage, TSP Traditional Deduction Amount, TSP Roth Deduction Amount, From Record Data As Of Date, From Record SCD Congressional, From Record SCD Leave, From Record SCD Retirement, From Record Is Transferee, From Record Military Service Years, From Record Military Service Months, From Record Military Service Days, From Record Long Term Care Insurance Premium Monthly, From Record SCD Law Fire ATC, TSP Catchup Contribution Amount, TSP Contribution Status, TSP Roth Catchup Contribution Amount, TSP Status Date, TSP Reelect Eligibility Date, FEHB Regular Eligibility Expiration Date, FEHB In Premium Conversion Plan Flag, FEHB Required To Provide Coverage To Dependent End Date, FEHB In Premium Conversion Plan Flag, FEHB Required To Provide Coverage To Dependent End Date, FEGLI Eligibility Due To Providing Medical Info Expire Date, FEGLI Eligibility Due Reinstatement Due To Break Expire Date, FEGLI Eligibility Due Reinstatement Due To Break Excluded Expire Date, FEGLI Eligibility Due DoD And Civilian Employees Affected By Pub Law 106398 And 110417 Expire Date, FEGLI Eligibility Due DoD And Civilian Employees Affected By Pub Law 106398 And 110417 Expire Date Included, Bank Name, Bank Account Number, Bank Routing Number, Federal Withholding, HCFSA Allotment Monthly, DCFSA Allotment Monthly, Lex

Version Date: October 1, 2022

Page 14 of 33

HCFA Allotment Monthly, FEDVIP Dental Premium Monthly, FEDVIP Vision Page 13 of 29 Premium Monthly, FEGLI Option Eligibility Expiration Date, OPM Work Schedule, Agency Organization Name, Agency Address, Agency City, Agency State, Agency Zip, Agency Country, Personnel Office Contact Name, Personnel Office Phone, Payroll Office Number, Payroll Office Contact Name, Payroll Office Phone, Is Educator, Educator Leave Balance Days, Payroll Provider, Servicing Personnel Office, From Date, To Date, Biweekly Tot, Pay Basis, Pay Rate, Pay Rate, Year, Earnings

3.2 How long is information retained?

*In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. **For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods.** The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented. If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

GRS 2.5, item 020: Individual employee separation files. It includes records not included in separating employee's eOPF, documenting individual employees' transfer to another Federal agency of office or voluntary, involuntary, disability, early retirement, or death separation from career, temporary, and political appointment service; and legal and financial obligations of government to employee to government. Retention is Temporary: Destroy 1 year after date of separation or transfer, but longer retention is authorized if required for business use.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner. Please work with the system Privacy Officer and VA Records Officer to answer these questions. This question is related to privacy control DM-2, Data Retention and Disposal.

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

GRS 2.5, item 020, <https://www.archives.gov/files/records-mgmt/grs/grs02-5.pdf>: Individual employee separation files. It includes records not included in separating employee's OPF, documenting individual employees' transfer to another Federal agency of office or voluntary, involuntary, disability, early retirement, or death separation from career, temporary, and political appointment service; and legal and financial obligations of government to employee to government.

3.3b Please indicate each records retention schedule, series, and disposition authority.

Retention is Temporary: Destroy 1 year after date of separation or transfer, but longer retention is authorized if required for business use.

3.4 What are the procedures for the elimination or transfer of SPI?

Explain how records are destroyed, eliminated or transferred to NARA at the end of their mandatory retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.? This question is related to privacy control DM-2, Data Retention and Disposal.

These determinations are made through records retention schedules and are required under 36 CFR 1234.10. Shredded by shredding company and accompanied by a certificate of destruction. Electronic records are deleted after one year.

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

VA has mitigated this risk through implementing FISMA Moderate 800.53 security controls. VA has implemented the required security and privacy controls according to NIST SP 800-53. 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.

Records go to Office of Personnel Management (OPM)

Live data will not be used for research, testing, or training.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

Consider the following FIPPs below to assist in providing a response:

Principle of Minimization: Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?

This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk: There is a risk that information could be retained for longer than necessary

Mitigation: These determinations are made through records retention schedules and are required under 36 CFR 1234.10. Shredded by shredding company and accompanied by a certificate of destruction. Electronic records are deleted after one year.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?

This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	List the purpose of the information being shared /received with the specified program office or IT system	List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system	Describe the method of transmittal
HR Smart	GRB is a comprehensive commercial retirement benefits calculator platform that is web based with capabilities to accurately compute various complex estimates needed in assisting employees with their retirement decisions. The calculator software is used for computing benefits and counseling employees under the Civil Service Retirement System (CSRS), Federal Employees Retirement System (FERS), the Federal Thrift Savings Plan and the Social Security program. Additionally, the application generates approved versions of form required for processing that meet standards and guidance set forth by the Office of Personnel Management (OPM). GRB will be receiving information from HR Smart and Defense Finance and Accounting System (DFAS).	Name, address, work email, SSN, DOB, dates of federal service, salary.	Data Feed

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: Disclosure of personally identifiable information, that if disclosed may expose the respondent/subject to financial loss or identity theft.

Privacy Risk: Disclosure of medical, personal, or other information that may compromise the individual’s reputation, circumstances, or safety.

Privacy Risk: Disclosure of participation in a study or activity, where knowledge of participation may adversely impact the individual’s reputation or circumstances. Mitigation:

Mitigation: Information will be secured on the system through access controls, personnel security awareness and training, regular auditing of information and information management processes, careful monitoring of a properly authorized information system, control of changes to the system, appropriate handling and testing of contingencies and contingency planning, ensuring that all users of the information system are properly identified and authorized for access, and that they are aware of the rules and acknowledge that fact, by ensuring that any incident is handled expeditiously, properly maintaining the system and regulating the environment the system operates in, controlling media, evaluating risks and planning for information management and information system operations, by ensuring that the system and any exchange of information is protected, by maintaining the integrity of the system and the information stored in it, and by adhering to the requirements established in applicable contracts.

Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.

This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	List the purpose of information being shared / received / transmitted with the specified program office or IT system	List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system	List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)	List the method of transmission and the measures in place to secure data
Defense Finance and Accounting System (DFAS)	GRB is a comprehensive commercial retirement benefits calculator platform that is web-based with capabilities to accurately compute various complex estimates needed in assisting employees with their retirement decisions. The calculator software is used for computing benefits and counseling employees under the Civil Service Retirement System (CSRS), Federal Employees Retirement System (FERS), the Federal Thrift Savings Plan and the Social Security program. Additionally, the application generates approved versions of form required for processing that meet standards and guidance set forth by the Office of Personnel Management (OPM). GRB will be receiving information from HR Smart and Defense Finance and Accounting System (DFAS).	Name, address, work email, SSN, DOB, dates of federal service, salary.	Required data element on OPM’s retirement forms, benefit election forms, and beneficiary forms. 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, and SORN 27VA047	Data Feed

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments. Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.

This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk: Privacy Risk: Disclosure of personally identifiable information, that if disclosed may expose the respondent/subject to financial loss or identity theft.

Privacy Risk: Disclosure of military service details that may compromise the individual's reputation, circumstances, or safety.

Privacy Risk: Disclosure of medical, personal, or other information that may compromise the individual's reputation, circumstances, or safety.

Privacy Risk: Disclosure of participation in a study or activity, where knowledge of participation may adversely impact the individual's reputation or circumstances.

Mitigation: Information will be secured on the system through access controls, personnel security awareness and training, regular auditing of information and information management processes, careful monitoring of a properly authorized information system, control of changes to the system, appropriate handling and testing of contingencies and contingency planning, ensuring that all users of the information system are properly identified and authorized for access, and that they are aware of the rules and acknowledge that fact, by ensuring that any incident is handled expeditiously, properly maintaining the system and regulating the environment the system operates in, controlling media, evaluating risks and planning for information management and information system operations, by ensuring that the system and any exchange of information is protected, by maintaining the integrity of the system and the information stored in it, and by adhering to the requirements established in applicable contracts.

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register,

Version Date: October 1, 2022

Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

Individuals are notified prior to data collection in accordance with VA policy and direction by VHA. VA 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). No information for GRB is collected directly from an individual.

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

N/A

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

SORN 27VA047, <https://www.govinfo.gov/content/pkg/FR-2012-07-02/pdf/2012-16167.pdf>

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.

VA 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). No information for GRB is collected directly from an individual.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

VA 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). No information for GRB is collected directly from an individual.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Has sufficient notice been provided to the individual?

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?

This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.

Follow the format below:

Privacy Risk: There is a risk that individuals are not notified their information is being collected.

Mitigation: VA 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). No information for GRB is collected directly from an individual.

Section 7. Access, Redress, and Correction

The following questions are directed at an individual’s ability to ensure the accuracy of the information collected about him or her.

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

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

*7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency’s FOIA/Privacy Act practices, but may also include additional access provisions. **For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency’s procedures. See 5 CFR 294 and the VA FOIA Web page at <http://www.foia.va.gov/> to obtain information about FOIA points of contact and information about agency FOIA processes.***

Individuals cannot change their information within GRB, they can only see their information. Employees can gain access through their eOPFs. Required data element on OPM’s retirement forms, benefit election forms, and beneficiary forms. 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.

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

Not exempt from the access provisions

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.

This is a Privacy Act system

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

If inaccurate or erroneous information is discovered prior to separation, the HR Specialist corrects the data. Employees would need to reach out to their servicing HR Office to correct their information.

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened.

This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Anytime there is a change to the eOPF an email is sent to the employee which provides an avenue for redress for corrections to contact their HR Representative.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.

Example: Some projects allow users to directly access and correct/update their information online.

This helps ensure data accuracy.

This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Redress is provided; they can see their information and they are provided the steps to have it corrected.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

Consider the following FIPPs below to assist in providing a response:

Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

Principle of Individual Participation: If access and/or correction is denied, then is the individual provided notice as to why the denial was made and how to challenge such a denial?

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?

This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk: There is a risk that individuals can't access or know how to correct.

Mitigation: They can see their information in GRB and provided notice when information is added to their eOPF and how to have information corrected by contacting their HR Representative.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system.

To obtain access to GRB you must be a VA employee to obtain user access. All access is provided by the system administrator who will determine whether access is user, HR access, or administrator 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. Employees will need to create a user account. They will be asked to verify their identity. Users are entered into the system by their SSNs. Roles are determined by system administrators located in the Retirement Shared Service Office (RSSO).

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

N/A system does not allow users from other agencies

8.1c Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

HR Manager, HR SCD-only, HR Read-only, None (no access to PII), Read-only

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

VA contractors do not have access to the system.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

Must complete VA Privacy and Cyber Security Awareness training which is required to be completed on a yearly basis.

VA Directive 6500 requires mandatory periodic training in computer security awareness and accepted computer security practices for all VA employees, contractors, and all other users of VA sensitive information and VA information systems. All members of the workforce are required to complete computer security training annually and must complete computer security awareness training before they can be authorized to access any VA computer system. Each site identifies personnel with significant information system security roles and responsibilities (i.e., management, system managers, system administrators, contracting staff, HR staff), documents those roles and responsibilities, and provides appropriate additional information system security training. Security training records will be monitored and maintained. The workforce will receive security awareness training annually as part of the Mandatory Training Program. In addition, the training for the tool will include awareness training regarding the possible existence of PII/PHI information submitted from the Veterans and eligible dependents. Each employee is asked to refresh their understanding of the appropriate way to handle the data.

8.4 Has Authorization and Accreditation (A&A) been completed for the system?

8.4a If Yes, provide:

1. The Security Plan Status: Approved
2. The System Security Plan Status Date: 10/05/2022
3. The Authorization Status: ATO
4. The Authorization Date: 08/07/2020
5. The Authorization Termination Date: 08/07/2023
6. The Risk Review Completion Date: 07/30/2020
7. The FIPS 199 classification of the system (LOW/MODERATE/HIGH): Moderate

Please note that all systems containing SPI are categorized at a minimum level of “moderate” under Federal Information Processing Standards Publication 199.

8.4b If No or In Process, provide your **Initial Operating Capability (IOC) date**.

N/A system currently in operation.

Section 9 – Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMAAS). This question is related to privacy control UL-1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1. (Refer to question 3.3.1 of the PTA)

GRB-e is a Software as a Service (SaaS) application powered the GRB Inc. GRB is a fully FedRAMP authorized system and it is hosted in vendor owned private cloud.

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting

information about PII/PHI from the contract). (Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Yes, Contract with GRB Inc. Contract number 36C77622C0162

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

CSP does not collect any ancillary data

9.4 NIST 800-144 states, “Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.” Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

See contract language below: The Contractor/Subcontractor must store, transport, or transmit VA sensitive information in an encrypted form, using VA-approved encryption tools that are, at a minimum, FIPS 140-2 validated. The Contractor/Subcontractor’s firewall and Web services security controls, if applicable, shall meet or exceed VA’s minimum requirements

9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as “Bots” or Artificial Intelligence (AI).

System does not use robotics processes

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

ID	Privacy Controls
AP	Authority and Purpose
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	Accountability, Audit, and Risk Management
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	Data Quality and Integrity
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	Data Minimization and Retention
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	Individual Participation and Redress
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	Security
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	Transparency
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information

ID	Privacy Controls
UL	Use Limitation
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

The individuals below attest that the information they provided in this Privacy Impact Assessment is true and accurate.

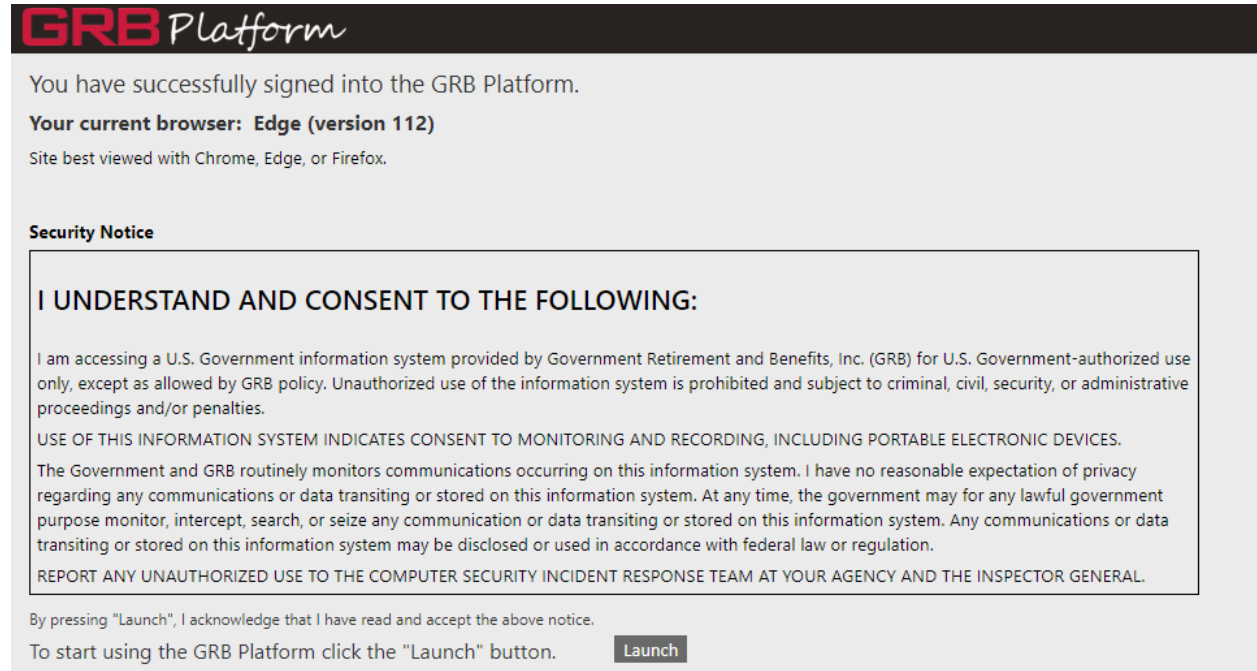
Privacy Officer, Kimberly Murphy

Information System Security Officer, Hurst McGraff

Information System Owner, Chino Walters

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy, a Privacy Act notice on forms). [RSSO-Government Retirements & Benefits \(sharepoint.com\)](#)



GRB Platform

You have successfully signed into the GRB Platform.

Your current browser: Edge (version 112)

Site best viewed with Chrome, Edge, or Firefox.

Security Notice

I UNDERSTAND AND CONSENT TO THE FOLLOWING:

I am accessing a U.S. Government information system provided by Government Retirement and Benefits, Inc. (GRB) for U.S. Government-authorized use only, except as allowed by GRB policy. Unauthorized use of the information system is prohibited and subject to criminal, civil, security, or administrative proceedings and/or penalties.

USE OF THIS INFORMATION SYSTEM INDICATES CONSENT TO MONITORING AND RECORDING, INCLUDING PORTABLE ELECTRONIC DEVICES.

The Government and GRB routinely monitors communications occurring on this information system. I have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system. At any time, the government may for any lawful government purpose monitor, intercept, search, or seize any communication or data transiting or stored on this information system. Any communications or data transiting or stored on this information system may be disclosed or used in accordance with federal law or regulation.

REPORT ANY UNAUTHORIZED USE TO THE COMPUTER SECURITY INCIDENT RESPONSE TEAM AT YOUR AGENCY AND THE INSPECTOR GENERAL.

By pressing "Launch", I acknowledge that I have read and accept the above notice.

To start using the GRB Platform click the "Launch" button.

HELPFUL LINKS

Record Control Schedules:

<https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf>

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

<https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf>

National Archives (Federal Records Management):

<https://www.archives.gov/records-mgmt/grs>

VHA Publications:

<https://www.va.gov/vhapublications/publications.cfm?Pub=2>

VA Privacy Service Privacy Hub:

<https://dvagov.sharepoint.com/sites/OITPrivacyHub>

Notice of Privacy Practice (NOPP):

[VHA Notice of Privacy Practices](#)

[VHA Handbook 1605.04: Notice of Privacy Practices](#)