SPLASH PAGE LANGUAGE

The completion of Veterans Affairs Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, system, or practice that collects or uses PII under the authority of the E-government Act of 2002 (44 U.S.C. § 208(b)) and VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment.

The PIA is designed to identify risk associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phases of the System Development Life Cycle (SDLC) of IT systems. It also ensures that privacy protections are built into an IT system during its development cycle. By regularly assessing privacy concerns during the development process, VA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements under the Federal Information Security Management Act (FISMA).

VA HANDBOOK 6508.1: “Implementation of Privacy Threshold Analysis and Privacy Impact Assessment,” July 2015, https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=810&FType=2

Please note that the E-government Act of 2002 requires that a PIA be made available to the public. In order to comply with this requirement PIA will be published online for the general public to view. When completing this document please use simple, straight-forward language, avoid overly technical terminology, and write out acronyms the first time you use them to ensure that the document can be read and understood by the general public.

Privacy Impact Assessment for the VA IT System called:

Platform Capability Delivery

Pension Automation

Benefits, Appeals, and Memorials Program (BAM)

Date PIA submitted for review:

11/29/2021

System Contacts:

System Contacts

Title	**Name**	**E-mail**	**Phone Number**	**Signature Required**
Privacy Officer	*Rita Grewal*	*Rita.Grewal@va.gov*	*202-632-7861*	*Yes*
Information System Security Officer	*Joseph Facciolli*	*Joseph.Facciolli@va.gov*	*215-842-2000 x2012*	*Yes*
Information System Owner	*Jim Rinehart*	*James.rinehart@va.gov*	*913-609-4495*	*Yes*
Data/Business/Information Owner[1]	*Click here to enter text.*	*Click here to enter text.*	*Click here to enter text.*	*No*

Abstract

The abstract provides the simplest explanation for "what does the system do?" and will be published online to accompany the PIA link.

Pension Automation (PA) seeks to automate the validation of data and business rules required during each step of the Pension claims workflow to reduce the duplication of effort across claims processing steps and manual processes. Goals of this system include:

** Reducing average days pending for a claim (ADP).*
** Increasing the number of claims that can be processed by the current workforce (Throughput).*
** Decreasing the inventory of claims pending completion (Inventory).*
** Maintaining or increasing processing accuracy (National Accuracy).*
** Enabling realignment of Human Resources from Pension claims to process to other critical areas.*

[1] VA DIRECTIVE 6508: Data Owner - Work with the POs, Program Managers, Project Managers, ISOs, System Managers, and System Developers to ensure that appropriate privacy protections related to data sensitivity are in place and indicated in their PIA submissions; Serve as point of contact for questions related to system data; Respond to questions from POs, Program Managers, Project Managers, ISOs, System Managers, and System Developers that are related to the PA submission.

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:

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *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.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *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?*

Pension Automation (PA) seeks to automate the validation of data and business rules required during each step of the Pension claims workflow to reduce the duplication of effort across claims processing steps and manual processes. Goals of this system include:

* Reducing average days pending for a claim (ADP).
* Increasing the number of claims that can be processed by the current workforce (Throughput).
* Decreasing the inventory of claims pending completion (Inventory).
* Maintaining or increasing processing accuracy (National Accuracy).
* Enabling realignment of Human Resources from Pension claims to process to other critical areas.

Pension Automation interacts with technical interfaces across Veterans Benefits Administration (VBA) to retrieve claim, Veteran, Claimant, and other critical data required to complete the claims process. The primary goal for PA is to run without user interaction, completing the claims process while retaining data integrity across all sub-systems within the Veteran VBA enterprise. The Office of Information and Technology's (OIT) maintains the system.

The system is hosted on Benefits Integration Platform (BIP). BIP is operated in a single instance of the VA Enterprise Cloud (VAEC) AWS GovCloud, deployed across three Availability Zones. The system is a minor application under the BIP Assessing system/project. It falls under the BIP Assessing Authority to Operate (ATO). All controls and hosting agreements with AWS are inherited from AWS VAEC GovCloud and BIP. BIP leverages the VAEC Cloud Service Provider (CSP) AWS GovCloud, which is FEDRAMP approved. VA Business Stakeholders of the BIP minor applications have ownership rights over data.

Pension Automation operates under the following legal authority:
- Title 38, United States Code, Sections 501(a), 1705, 1710, 1722, and 5317

Version Date: January 2, 2019
Page 3 of 19

- 5 U.S.C. 552, "Freedom of Information Act," c. 1967
- 5 U.S.C. 552a, "Privacy Act," c. 1974
- OMB Circular A-130, Appendix III, “Security of Federal Automated Information Systems”
- Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act)
- Federal Information Security Management Act (FISMA) of 2002
- OMB M-03-22, “OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002,
- VA Directive and Handbook 6502, Privacy Program

The system processes PII/PHI related to veterans, spouses, and dependents.

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 (III), 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://vaww.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:

☒ Name
☒ Social Security Number
☒ Date of Birth
☐ Mother’s Maiden Name
☒ Personal Mailing Address
☒ Personal Phone Number(s)
☐ Personal Fax Number
☒ Personal Email Address
☒ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☒ Financial Account Information
☒ Health Insurance Beneficiary Numbers Account numbers

☒ Certificate/License numbers
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☐ Current Medications
☒ Previous Medical Records
☒ Race/Ethnicity

☒ Tax Identification Number
☒ Medical Record Number
☒ Gender
☐ Integration Control Number (ICN)
☒Military History/Service Connection
☒ Next of Kin

☒ Other Unique Identifying Information (list below)
Veteran File Number
Veteran Service Number

PII Mapping of Components

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

PII Mapped to Components

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.

PII Mapped to Components

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**
VBMSUI	Yes	Yes	Veteran File Number Veteran SSN Veteran First Name Veteran Last Name Claimant File Number Claimant SSN Claimant First Name Claimant Last Name	All data collected is required to evaluate pension eligibility so that VA can award the appropriate benefits to claimants and dependents.	DB uses strong authentication and authorization. Only approved user accounts have access. System monitoring and alerts are enabled.

ClaimAutomator	Yes	Yes	Veteran File Number Veteran SSN Veteran First Name Veteran Last Name Claimant File Number Claimant SSN Claimant First Name Claimant Last Name Address information	Data collected is used for electronic documents and letters sent to the claimant.	DB uses strong authentication and authorization. Only approved user accounts have access. System monitoring and alerts are enabled.
Camunda	Yes	Yes	Veteran, Claimant and Dependent information • Name • Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Email Address • Financial Account Information • Tax Identification Number • Medical Record Number • Military Service History • Other Unique Identifying Number (File Number and Participant ID)	All data collected is required to evaluate pension eligibility so that VA can award the appropriate benefits to claimants and dependents.	DB uses strong authentication and authorization. Only approved user accounts have access. System monitoring and alerts are enabled.

			• Date of death and associated information on death certificates		

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

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?

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 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

All data collected is required to evaluate pension eligibility so that VA can award the appropriate benefits to Veterans and Claimants.

- Benefits Processing Data (BPD) provides extracted data from VA forms and submitted evidence.
- The Claims API provides the ability to read and update claim data.
- Benefits Gateway Services (BGS) provide veteran and dependent profile information, address information, military service history, development actions, ratings information and award information.
- Veteran Benefits Management System (VBMS) is the primary user interface for VBA users that process Compensation and Pension claims. VBMS provides claim and document-related information.
- DocGen service generates Portable Document Format (PDF) documents after the process has been complete.
- The Service-Connected Death Classifier determine if the cause of death meets business criteria for eligibility.

- Mail Automation System (MAS) extracts data from VA claim forms and associated documents so that the data can be used by Pension Automation.
- The VBMS eFolder stores electronic documents generated by Pension Automation.
- Package Manager, also known as Centralized Benefits Communication Management (CBCM), provides an interface to distribute packages that are sent through the CBCM vendor for printing and postal mail.

1.3 How is the information collected?

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 technology used in the storage or transmission of information in identifiable form?

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.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

All information is collected electronically via systems integration.

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

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.

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.
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

The system evaluates all data through a series of data validation routines and business rule checks as part of the automation process. Various checks are in place to ensure data accuracy. Daily executive reports and operational reports are provided to multiple groups within VA.

All decisions are logged and are reviewed when discrepancies are reported. The support team has a well-defined production defect process to resolve issues and research potential issues.

Periodic audits by subject matter experts are conducted to review Pension Automation results.

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

- 5 U.S.C. § 552a, Freedom of Information Act of 1996, As Amended By Public Law No. 104---231, 110 Stat. 3048
- 5 U.S.C. § 552a, Privacy Act of 1974, As Amended
- Public Law 100---503, Computer Matching and Privacy Act of 1988
- Privacy Act of 1974; U.S Code title 5 USC section 301 title 38 section 1705, 1717, 2306-2308 & Title38, US Code section 7301 (a) and Executive Order 9397
- OMB Circular A---130, Management of Federal Information Resources, 1996
- OMB Memo M---03---22, OMB Guidance for Implementing the Privacy Provisions
- OMB Memo M---07---16, Safeguarding Against and Responding to the Breach of PII
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- State Privacy Laws
- The legal authority is 38 U.S.C 7601-7604 and U.S.C 7681-7683 and Executive Order 9397

1.6 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>

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.

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

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

<u>Principle of Minimization:</u> *Is the information directly relevant and necessary to accomplish the specific purposes of the program?*

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

<u>Principle of Data Quality and Integrity:</u> *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: Incorrect data could be sent to Pension Automation when evaluating claims
Mitigation: System controls validate data inputs and there many business rules are executed against the data prior to any decisions. Additionally, there is a full audit trail of system actions and decision. All data is sourced from trusted VA systems that also have data integrity and privacy controls.

Privacy Risk: Letters sent to incorrect addresses
Mitigation: All addresses are sourced from the VA systems of record, which have data integrity and privacy controls.

Privacy Risk: System is compromised, and data is stolen
Mitigation: The system uses strong security controls. The Department of Veterans Affairs applies consistent security guidance to centralize and standardize account management, network access control, database security, vulnerability scanning and remediation.

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.

Pension Automation (PA) seeks to automate the validation of data and business rules required during each step of the Pension claims workflow to reduce the duplication of effort across claims processing steps and manual processes. Goals of this system include:

** Reducing average days pending for a claim (ADP).*
** Increasing the number of claims that can be processed by the current workforce (Throughput).*
** Decreasing the inventory of claims pending completion (Inventory).*
** Maintaining or increasing processing accuracy (National Accuracy).*
** Enabling realignment of Human Resources from Pension claims to process to other critical areas.*

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

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.

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 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.
This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

Monitoring is accomplished using software tools called Kubernetes, Prometheus, Grafana and Kibana. The system is configured to monitor CPU, memory, I/O, API request/response latency and API HTTP response codes. Alerts are configured to notify administrators if the application is having resource (e.g. memory or CPU) issues.

The system uses a process automation engine to make decisions about the claim. The result is either a pension award denial, grant or “off-ramp,” which means the system needs more information. Results are only used for automating the pension claim process.

2.3 How is the information in the system secured?

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

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

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

This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest

All data is encrypted during transit using SSL. Data at rest is only accessible by system administrators and privileged users that are granted access through a standard approval process. Data at rest is obfuscated.

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u> How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. <u>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.</u>

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.

Add answer here:

Access to PII is determined by IT role (System Administrator) and privileged users for support scenarios. Privileged users are granted read access using a standard approval process that requires manager level and system owner approvals.

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

Veteran, Claimant and Dependent information

- Name
- Social Security Number
- Date of Birth
- Personal Mailing Address
- Personal Phone Number(s)
- Personal Email Address
- Financial Account Information
- Tax Identification Number
- Medical Record Number
- Military Service History
- Other Unique Identifying Number (File Number and Participant ID)
- Date of death and associated information on death certificates

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. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.
This question is related to privacy control DM-2, Data Retention and Disposal.

VA Form Data is retained indefinitely.
RETENTION AND DISPOSAL:
Paper records and information are maintained and disposed of in accordance with records disposition authority approved by the Archivist of the United States.
See SORN: https://www.govinfo.gov/content/pkg/FR-2010-10-21/pdf/2010-26490.pdf

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so, please indicate the name of the records retention schedule.

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.
This question is related to privacy control DM-2, Data Retention and Disposal.

Retention Schedule SORN: https://www.govinfo.gov/content/pkg/FR-2010-10-21/pdf/2010-26490.pdf

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the 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

Until a retention schedule is approved or needed, no data will be eliminated. If elimination is needed ad hoc, the underlying data store would be updated to remove desired SPI.

RETENTION AND DISPOSAL:
Paper records and information are maintained and disposed of in accordance with records disposition authority approved by the Archivist of the United States.
See SORN: https://www.govinfo.gov/content/pkg/FR-2010-10-21/pdf/2010-26490.pdf

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. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?
This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

Yes. No PII data is used in testing or development environments. Only production system admins have access to production environments.

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.

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: Excessive information stored

Mitigation: Partners that request data to be stored must adhere to the principle of minimalization regarding the data being requested for storage.

Privacy Risk: Indefinite retention

Mitigation: Without a retention schedule, ad hoc removals would have to occur when needed.

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***
Veterans Benefits Administration / Office of Information and Technology	VBMS	• Veteran File Number • Veteran SSN • Veteran First Name • Veteran Last Name • Claimant File Number • Claimant SSN • Claimant First Name	Receives data via secure SQL Query

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***
		Claimant Last Name	
Veterans Benefits Administration / Office of Information and Technology	BGS	Veteran, Claimant, Dependent and Power of Attorney and Fiduciary information • Veteran Profile • Claimant Profile • Fiduciary Profile • Power of Attorney Profile • File Number • SSN • Claim Award Information • Claim Rating Information • Burial Information • Military Service History • Power of Attorney Information • Claim Tracked Items • Claim Development Notes Mailing Address	Receives and updates data via HTTPS /SOAP Request/Response. Secured by SAML and HTTPS.
Veterans Benefits Administration / Office of Information and Technology	BIP BPDS API	Veteran, Claimant and Dependent information • Name • Social Security Number • Date of Birth • Mother's Maiden Name • Personal Mailing Address	Receives data via HTTPS Request/Response (JSON data format)

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***
		• Personal Phone Number(s) • Personal Fax Number1 • Personal Email Address • Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Financial Account Information • Health Insurance Beneficiary Numbers • Account numbers • Certificate/License numbers • Vehicle License Plate Number • Internet Protocol (IP) Address Numbers • Current Medications • Previous Medical Records • Race/Ethnicity • Tax Identification Number • Medical Record Number • Other Unique Identifying Number Date of death and associated information on death certificates	
Veterans Benefits Administration / Office of Information and Technology	BIP DocGen API	• Burial letter, development letter, rating code sheet, rating narrative and award letter information • Veteran Profile	Receives and sends data via HTTPS Request/Response (JSON data format)

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*
		• Claimant Profile • Fiduciary Profile • Power of Attorney Profile • Mailing Addresses File Number	
Veterans Benefits Administration / Office of Information and Technology	BIP Classifier	Date of death and associated information on death certificates	Receives and sends data via HTTPS Request/Response (JSON data format)
Veterans Benefits Administration / Office of Information and Technology	VBMS (eFolder and Package Manager)	• Burial letter, development letter, rating code sheet, rating narrative and award letter information • Veteran Profile • Claimant Profile • Fiduciary Profile • Power of Attorney Profile • Mailing Addresses File Number	Receives and updates pdf via HTTPS /SOAP Request/Response. Secured by SAML and HTTPS.
Veterans Benefits Administration / Office of Information and Technology	Mail Automation System (MAS)	• Veteran File Number • Veteran SSN • Veteran First Name • Veteran Last Name • Claimant File Number • Claimant SSN • Claimant First Name • Claimant Last Name	Receives and sends data via HTTPS Request/Response (JSON data format)

4.2 <u>PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure</u>

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

Follow the format below:

Privacy Risk: The privacy risk associated with accessing and maintaining SPI is that this data may be disclosed to individuals who do not require access, which would increase the risk of the information being misused.

Mitigation:

Safeguards are implemented to ensure data is not sent to unauthorized VA employees, including employee security and privacy training, and required reporting of suspicious activity. Use of secure passwords, access for need to know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized by the system. Further, SPI is always encrypted while in transit.

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***
NA	NA	NA	NA	NA

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:
Not applicable, as there is no sharing of information outside of VA with external parties.

Mitigation:
Not applicable, as there is no sharing of information outside of VA with external parties.

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 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?

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. If notice was provided in the Federal Register, provide the citation.

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

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. This question is 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.

Pension Automation does not collect information from individuals. Individuals are provided notice when they submit claim forms.

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

Pension Automation does not collect information from individuals. Individuals are provided notice when they submit claim forms and can choose not to provide information.

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

Pension Automation does not collect information from individuals directly. Right to consent and privacy disclaimers are listed on claim forms.

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.

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: NA

Mitigation: NA

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?

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.

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).

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 question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

Requests for records can be submitted electronically at ncafoia@va.gov

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.

VHA Handbook 1605.1 Appendix D 'Privacy and Release Information', section 7(b) states the rights of the Veterans to request access to review their records. VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to and reviewed by the System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted.

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.

Individuals are not notified if there is missing or inaccurate information in their record. An individual who wishes to determine whether a record is being maintained under his or her name in Pension Automation or wishes to determine the contents of such records should submit a written request or apply in person to the VA facility where the records are located. Requests should contain the full name, address and telephone number of the individual making the inquiry. (Per 58VA21/22/28 SORN)

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

Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.

Veterans and other beneficiaries may contact their supporting VA regional office or VHA center to learn how to access, correct, or contest their information.

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.

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 a system provides incorrect information to Pension Automation, which may lead to an incorrect pension eligibility decision.

Mitigation: Pension Automation includes data validation and provides error messages to Veteran Service Representatives via the VBMS user interface if data is invalid or fails business rule processing. In addition, nightly reports are provided to operations personnel for review. Finally, periodic audits are conducted by the VBA Pension & Fiduciary team to ensure eligibility decisions and outcomes are accurate. All defects are reported to application support and delivery teams, which have a defect resolution process.

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?

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

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?

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.

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

System Administrators will have access to the system. The System Administrators are not primary users of the Pension Automation system, nor do they develop components for the system.

Privileged users may be granted read access for system support. The support role cannot change data in the system

All access requests must be sent using a standard systems access request and must be approved by the System Owner and Production Operations staff.

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.

Contractor teams support the production environment and as such have access to the Pension Automation system. This includes PII and VA Sensitive Information. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of Behavior training via the VA's Talent Management System (TMS). The System Administrators will maintain users, update applications and components, introduce new functionality, govern deployment activities, and ensure user operability. The System Administrators are not primary users of the Pension Automation system, nor do they develop components for 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.

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training that all personnel must complete via the VA's Talent Management System 2.0 (TMS). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the privacy and security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS 2.0 system.

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

If Yes, provide:

1. *The Security Plan Status,*
2. *The Security Plan Status Date,*
3. *The Authorization Status,*
4. *The Authorization Date,*
5. *The Authorization Termination Date,*
6. *The Risk Review Completion Date,*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

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

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

No. The current ATO for Pension Automation in in progress.

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).

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.

Yes, the system is hosted on VA Enterprise Cloud (VAEC)

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)

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

N/A

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.

N/A

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.

N/A

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).

N/A

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
UL	**Use Limitation**

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

Signature of Responsible Officials

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

RITA K GREWAL 114938

Digitally signed by RITA K GREWAL 114938
Date: 2021.12.06 10:55:40 -05'00'

Privacy Officer, Rita Grewal

Joseph Facciolli 148552

Digitally signed by Joseph Facciolli 148552
Date: 2021.12.03 14:29:12 -05'00'

Information Systems Security Officer, Joseph Facciolli

James B. Rinehart 3592539

Digitally signed by James B. Rinehart 3592539
Date: 2021.12.06 10:24:38 -06'00'

Information System Owner, James Rinehart

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).