Privacy Impact Assessment for the VA IT System called:

INSURANCE PAYMENT SYSTEM

INSURANCE CENTER
VBA INSURANCE PROGRAM

Date PIA submitted for review:

06/30/21

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Rita Grewal	Rita.Grewal@va.gov	202-632-7861
Information System Security Officer (ISSO)	Richard Powell	Richard.Powell@va.gov	215-842-2000 ext. 4353
Information System Owner	William Wigton	William.Wigton@va.gov	817-999-6851

Abstract

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

The Insurance Payment System (IPS) is the core back end of the Insurance system. The Insurance schedule runs every workday to update veterans' master records. Records are updated on their anniversary date, or in response to events (such as lapse), or when transactions are entered by Insurance Center staff. IPS produces disbursement files for life insurance dividends and award payments. The disbursements can be made by check, direct deductions (DD), or electronic funds transfer (EFT) and the insurance payment processes interface with Department of Defense (DOD) and Social Security Administration (SSA) systems processes. The IPS system also sends the disbursement files to Treasury every day, to produce checks and direct deposits. IPS generates about 750,000 mail items every year.

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?*

The mission of the Veterans Benefits Administration (VBA) Insurance program is to provide life insurance benefits to Veterans and service members that are not available, under present guidelines, from the commercial insurance industry. Veterans and service members may not be able to obtain insurance from private companies because of the extra risks involved in military service or a service-connected disability. VBA's Insurance Service Division administers six government life insurance programs that provide approximately $30 billion in coverage to over two million policyholders.
Approximately 100,000 death cases are adjudicated annually, most resulting in lump sum payments. More than 80,000 beneficiaries of deceased Veterans receive monthly annuity checks in lieu of a lump sum payment of the policy proceeds. The programs disburse nearly $2 billion annually in dividends and death/disability awards.

Insurance Payment System, hosted on the Insurance LAN, which is located at the Philadelphia Information Technology Center, is the oldest of the Insurance business systems. It generates six million pieces of mail annually and produces disbursement files and other external interfaces. Insurance Payment System includes batch subsystems: "Inforce" (current policyholders), "Awards" (recipients), "Actuarial" (insurance statistical calculations), and an "On-Line" subsystem. The On-Line subsystem supports Insurance inquiry and Data entry and is the vehicle for providing Insurance data to Veterans Service Representatives (VSRs) at VA Regional Offices (ROs). The subsystems include programs that post premiums from multiple sources, including pre-authorized debits (PAD) from a checking account and deductions from Veteran's benefits (DFB), and maintain accountability for money owed to Veterans whose locations are unknown.
Insurance Payment System produces disbursement files for life insurance dividends and award payments. The disbursements can be made by check, direct deductions (DD), or electronic funds transfer (EFT) and the insurance payment processes interface with Department of Defense (DOD) and Social Security Administration (SSA) systems processes.

Insurance Payment System currently only processes disbursements to Veterans of World War II and the Korean War.

The Secretary of Veterans Affairs established these guidelines pursuant to the authorities in and requirements of Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources," and the authorities contained under Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of

Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency Agreements," also known as the "Economy Act." These guidelines assist in the implementation of these statutes. Insurance Payment System is covered under SORN VA 36VA29.

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.

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
- ☐ Other Unique Identifying Information (list below)

<<Add Additional Information Collected But Not Listed Above Here (For Example, A Personal Phone Number That Is Used As A Business Number)>>

PII Mapping of Components

Insurance Payment System consists of 4 key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Insurance Payment System 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.

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
Inforce	Yes	Yes	• Name • Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number • Financial Account Information	Maintain policy holder financial and contact information	Database encrypted; secure FTP and connect:direct (FIPS 140-2)
Awards	Yes	Yes	• Name • Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number • Financial Account Information	Disbursement for recipients (Veterans and Beneficiaries)	Database encrypted; secure FTP and connect:direct (FIPS 140-2)
Actuarial	No	N/A	N/A	N/A	N/A

Online	Yes	Yes	• Name • Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number • Financial Account Information	Maintain policy holder financial and contact information	Database encrypted; SSL Connection enforced

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.

Insurance Payment System includes batch subsystems: "Inforce" (current policyholders), "Awards" (recipients), "Actuarial" (insurance statistical calculations), and an "On-Line" subsystem. The On-Line subsystem, Insurance Terminal System (ITS), supports insurance inquiry and data entry and is the vehicle for providing insurance data to Veterans Service Representatives (VSRs) at VA Regional Offices (ROs). The subsystems include programs that post premiums from multiple sources, including pre-authorized debits (PAD) from a checking account and deductions from Veteran's benefits (DFB), and maintain accountability for money owed to Veterans whose locations are unknown. The Insurance Payment System interfaces with the Financial Management System (FMS), Benefits Delivery Network (BDN) and Veterans Insurance Claims Tracking and Response System (VICTARS).

The following are the internal subsystems within IPS:

- Inforce - Stores and updates information about living policyholders, including addresses and bank data. Inforce processes payments received from various sources via personal check, deduction from benefits, and pre-authorized debits from bank accounts. Inforce performs annual dividend processing, and controls loan/lien and liabilities handling for VA indebtedness.

- Awards - Controls the processing and initiation of lump-sum and recurring payments to insurance beneficiaries and certain classes of insured Veterans.
- Actuarial - Collects statistical data daily from the Inforce and Awards subsystems and aggregates the data weekly, monthly, quarterly, and annually.
- Insurance On-Line - Also known as the Insurance Terminal System (ITS), it provides claims adjusters with inquiry and data entry capabilities for managing individual case file data used by the Inforce and Awards subsystems. Insurance On-line interfaces with Insurance Self Service and Insurance Unclaimed Liabilities but is functionally separate and used for internal purposes only.

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.

Information is collected by external systems (please refer to section 5) and imported via batch processing but is not subject to the Paperwork Reduction Act.

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.

Data is checked for completeness by system audits, manual verifications, and annual questionnaires through automated Veterans letters. These letters ask specific questions for verification based on the existing entitlement or benefit the Veteran is receiving. The correspondence with each Veteran is then used to update the data. All collected data are matched against supporting claims documentation submitted by the Veterans.
Certain data such as Social Security Number (SSN) is verified with the Social Security Administration. Prior to any award or entitlement authorization(s) by the VBA the Veteran's record is manually reviewed and data validated to ensure correct entitlement has been approved.

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 Secretary of Veterans Affairs established these guidelines pursuant to the authorities in and requirements of Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources," and the authorities contained under Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency Agreements," also known as the "Economy Act." These guidelines assist in the implementation of these statutes.

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.

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:
The IPS collects both personally identifiable information (PII) and a variety of other sensitive personal information (SPI). Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional, or financial harm may result for the individuals affected.

Mitigation:
IPS employs a variety of security measures designed to ensure that the information is not inappropriately disclosed or released. These measures include access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance.

Accessing the data on the Insurance Payment Systems requires access approval through Security Management System (SMS) for business users (ePAS system for system administrators); management generates a 9957 to create an account in Computer Associates Top Secret program that maintains security controls on the Mainframe. Access to the mainframe creates an audit log that is maintained by the ITOPS IO Security Management. Any unauthorized access to the system will be flagged and create an incident from Security Management.

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 intended use of the Veterans' and service members' information is to provide life insurance benefits to Veterans and service members that are not available, under present guidelines, from the commercial insurance industry. Veterans and service members may not be able to obtain insurance from private companies because of the extra risks involved in military service or a service-connected disability.

Other use of the Veteran's and Veteran's family or guardian's (spouse, children, parents, grandparents, etc.) information is to determine eligibility and entitlement for VA compensation and pension benefits and also designate a guardian to manage the VA compensation and pension benefits of those individuals who are not competent to manage their own funds for VA entitlement purposes.

- Name –Required to identify account holders, send correspondences, and address customers when communicating on the phone.
- Social Security Number – Required to match records with Social Security Death Master File
- Date of Birth – Required to calculate age to determine eligibility for Insurance Programs and determine premium rates.
- Mailing Address – Required to mail billing, payment, and other general correspondences.
- Zip Code – Required to mail billing, payment, and other general correspondences.
- Phone Number(s) – Required to call Policyholders or Beneficiaries when developing claims or resolving customer service inquiries.
- Financial Account Information – Required to maintain balances for cash value, loans, liens, or dividend credit.

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

Internal financial and actuarial reports are generated by in-house software written within the application by local developers who are VA OI&T employees. External tools, such as Excel, may be used to further analyze the data to perform more extensive calculations and analysis beyond what's provided in the standard reports. These reports are used by Insurance Operations and Program Management to perform accounting reconciliations and to complete actuarial studies of the financial integrity of the Insurance Program. The actuarial studies are used to make recommendations for interest rates, dividend rates, and buying or selling securities in reserve funds.

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?

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

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information. 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. 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.

All users must register to access the IPS application. Internal users are validated against the Windows Active Directory user database. The data requests are delivered through a Secure Socket Layer (SSL) connection.
All internal employees with access to Veterans information are required to have the appropriate level background investigation and must complete the VA Privacy and Information Security awareness training and rules of behavior annually.

Disciplinary actions, depending on the severity of the offense, include counseling, loss of access, suspension and possibly termination.

VA Employees and Contractors are given access to Veterans data through the issuance of a user ID and password. This ensures the identity of the user by requiring two-factor authentication. The user ID limits the access to only the information required to enable the user to complete their job. External users are vetted through their lender/servicer organization. An administrator within the organization authorizes the initial user registration and then validates their continued access every 90 days.

The official system of records notice (SORN) 36VA29 dated 10/22/2010 for "Veterans and Uniformed Services Personnel Programs of U.S. Government Life Insurance-VA can be found online at:
http://www.gpo.gov/fdsys/pkg/FR-2010-10-22/pdf/2010-26491.pdf

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
- Mailing Address
- Zip Code
- Phone Number(s)
- Financial Account Information

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.

Currently the retention period on documents set to "0", documents never gets deleted. This is because requirements were structured to adhere to the paper requirements and for Insurance Payment System to become of a system of record. 75 FR 65405 published October 22, 2010.
http://www.gpo.gov/fdsys/pkg/FR-2010-10-22/pdf/2010-26491.pdf

The data retention period for Veterans data is contained in RCS VBA-1, Part1, Item Number 08-065.000 and subparagraphs, which states "Destroy files data in accordance with system design." Record information pertaining to service members will continue to be maintained into perpetuity. Records are archived in accordance with retention policies and procedures.

- RCS 10-1 link for VHA: http://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

RCS VB- Part II Revised for VBA: http://www.benefits.va.gov/warms/docs/admin20/rcs/part2/vb-1partii.doc

- National Archives and Record Administration: www.nara.gov

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.

VBA Records Management, Records Control Schedule VB-1, Part 1, Section IX, INSURANCE as authorized by NARA
https://www.benefits.va.gov/WARMS/docs/regs/RCS_I.doc

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

Data is not eliminated. It is controlled in accordance with NARA control schedules determined by agency involved. VA Handbook 6300.1, Records Management Procedures, explains the Records Control Schedule procedures. Operating units will follow VA policy.

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

Risk minimized by test databases not containing true Veterans data.

3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

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:

<u>Principle of Minimization:</u> 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?

<u>Principle of Data Quality and Integrity:</u> 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:

Insurance Payment system is the Master System of Record for the Insurance Service Line; therefore, records are maintained in IPS indefinitely. Records remain active on the mainframe until the award is fully paid. The possibility of a data breach or system compromise increases when maintaining records for an extended period.

Mitigation:

After an award is paid, the inactive records are archived to tape and taken to the off-sight location in Iron Mountain. Active records that remain on the mainframe will be secured and monitored in accordance with utilizing VA policy. RCS VB- Part II Revised for VBA: http://www.benefits.va.gov/warms/docs/admin20/rcs/part2/vb-1partii.doc

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 3.10 (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 shared/received with the Program Office or IT system***	***Describe the method of transmittal***
Office of Management: Financial Management System (FMS)	Financial reporting	Summary Level Accounting Information	IBM Connect Direct 5.0.0
Veterans Benefits Administration: Benefits Delivery Network (BDN)	Receive deduction benefit information	Name, Social Security Number, Date of Birth; Mailing Address/Veterans or Primary Subject's Personal Contact Information (name, address, telephone, etc); and Financial Account Information	IBM Connect: Direct 5.0.0
Insurance Center: Veterans Insurance Claims Tracking and Response System (VICTARS)	Replication of data	Name, Social Security Number, Date of Birth; Mailing Address/Veterans or Primary Subject's Personal Contact Information (name, address, telephone, etc); and Financial Account Information	Secure file transfer protocol (SFTP).

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

Follow the format below:
Privacy Risk:

There is a risk that data contained in the Insurance Payment System may be shared with unauthorized individuals or that those individuals, even when permitted to access the data, may share it further with other individuals.

Mitigation:
Information is transferred in a site-to-site, two-way, FIPS 140-2 complaint VPN connection where exchange secured file transfers via internet using Attachmate FIPS 140-2 complaint Secure File Transfer Protocol (SFTP) software.

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 3.11 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	***List the purpose of information being shared / received /***	***List the specific PII/PHI data elements that are shared/received***	***List the legal authority, binding agreement,***	***List the method of transmission and the measures in***

shared/received with	*transmitted with the specified program office or IT system*	*with the Program or IT system*	*SORN routine use, etc. that permit external sharing (can be more than one)*	*place to secure data*
Defense Finance and Accounting Services (DFAS)	Department of Defense (DoD)	The files that are exchanged between DFAS and the VA include PII information including the members' (Name, Social Security Number, Date of Birth; Mailing Address/Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc); and Financial Account Information.	Data from the DFAS to VA will be encrypted and transferred using Connect: Direct Secure Plus File Transfer software through a VA Transport Layer Protocol site-to-site VPN tunnel, which provides FIPS 140-2 compliant	Local ISA/MOU
Death Master File (DMF)	Social Security Administration (SSA)	The files that are exchanged between SSA and the VA include PII information including the members' (Full Name, Full Social Security Number, Date of Birth; Mailing Address/Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc); and Financial Account Information.	Two-way data being passed between SSA and VA will be encrypted and transferred using Connect:Direct Secure plus file transfer through a FIPS 140-2 compliant VA transport layer protocol site to site VPN tunnel.	Local ISA/MOU
Fiscal Service	Department of the Treasury Bureau of the Fiscal Service	The files that are exchanged between Treasury and the VA include PII information including the	Data from the Fiscal Service to VA will be transferred via a VPN tunnel using Connect: Direct	Local ISA/MOU

		members' (Full Name, Full Social Security Number, Date of Birth; Mailing Address/Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc.); Family Relation (spouse, children, parents, grandparents, etc.); Service Information; Benefit Information and Financial Account Information.	Secure Plus software.	

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

- The information with each application is categorized in accordance with FIPS 199 and NIST SP 800-60. As part of the categorization any PII is identified.
- The VA has policies which direct and guide the activities and processes performed by the VA. The policies are periodically reviewed to ensure completeness and applicability.
- The NIST SP 800-53 controls are selected based on the categorization. The controls provide protection for Veteran PII while developed or stored by an application or IT system, physically transported, between facilities, least privilege, stored offsite, or transmitted between IT centers.
- Internal protection is managed by access controls such as user authentication (user IDs, passwords, and Personal Identification Verification (PIV)), awareness and training, auditing, and internal network controls. Remote protection is provided by remote access control, authenticator management, audit, and encrypted transmission.

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:
There is a risk that data contained in the Insurance Payment System (IPS) may be shared with unauthorized individuals or that those individuals, even when permitted to access the data, may share it further with other individuals.

Mitigation:
- Information is transferred in a site-to-site, two-way, FIPS 140-2 compliant VPN connection where exchange secured file transfers via internet using Attachmate FIPS 140-2 compliant Secure File Transfer Protocol (SFTP) software.
- Trusted Behavior Expectation: There is a Memorandum of Understanding (MOU) expected to engage the external party appropriate protective measures as not to subject VA data to undue risk. The external party comply with the Privacy Act and Trade Secrets Act (18 U.S.C. § 1905) and the Unauthorized Access Act (18 U.S.C. §§ 2701 and 2710). Users are expected to protect VA information resources, and VA system and users are expected to protect VA information resources in accordance with the Privacy Act and Trade Secrets Act (18 U.S.C. § 1905) and the Unauthorized Access Act (18 U.S.C. §§ 2701 and 2710)

- Audit Trail Responsibilities: External party is responsible for auditing application processes and user activities involving the hard copy and imaged data, and access to the Secure FTP server where VA sensitive data is stored. Additionally, uploaded data through the interconnection should have sufficient granularity and auditing identifiers to allow successful investigation and possible prosecution of wrongdoers. Activities that will be recorded include event type, date, and time of event, user identification, workstation identification, and security actions security officers. Audit logs will be retained for one (1) year or for the duration specified in the contract and provided to VA upon request.

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.

The Department of Veterans Affairs does provide public notice that the system does exist. This notice is provided in 2 ways:

1. The System of Record Notice (SORN) "Veterans and Uniformed Services Personnel Programs of US Government Life Insurance – VA" 36VA29/83 FR 44407 dated 08/30/2018

This SORN can be found online at:
(https://www.oprm.va.gov/privacy/systems_of_records.aspx).
https://www.govinfo.gov/content/pkg/FR-2018-08-30/pdf/2018-18789.pdf

2. This Privacy Impact Assessment (PIA) also serves as notice of the PITC Insurance Payment System. As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register.

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

N/A. Veterans do not directly provide information to the system. All information is collected by external systems.

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

While individuals may have the ability to consent to various uses of their information at the VA, they are not required to consent to the use of their information as part to determine eligibility and entitlement for VBA's Insurance Service Division benefits.

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:
There is a risk that members of the public may not know that the Insurance Payment System exists within the Department of Veterans Affairs.

Mitigation:
The VA mitigates this risk by providing the public with two forms of notice that the system exists, as discussed in detail in question 6.1, including the Privacy Act statement and a System of Record Notice.

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.

Individuals wishing to obtain more information about access, redress and record correction of Insurance Payment System should contact the Department of Veteran's Affairs regional offices as directed in the System of Record Notice (SORN) "Veterans and Uniformed Services Personnel Programs of US Government Life Insurance – VA" 36VA29/83 FR 44407 dated 08/30/2018
This SORN can be found online at:
(https://www.oprm.va.gov/privacy/systems_of_records.aspx).
https://www.govinfo.gov/content/pkg/FR-2018-08-30/pdf/2018-18789.pdf

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.

Individuals wishing to obtain more information about access, redress and record correction of Insurance Payment System should contact the Department of Veteran's Affairs regional offices as directed in the System of Record Notice (SORN) "Veterans and Uniformed Services Personnel Programs of US Government Life Insurance – VA" 36VA29/83 FR 44407 dated 08/30/2018
This SORN can be found online at:
(https://www.oprm.va.gov/privacy/systems_of_records.aspx).

https://www.govinfo.gov/content/pkg/FR-2018-08-30/pdf/2018-18789.pdf

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.

Individual wishing to obtain more information about access, redress and record correction of Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records should contact the Department of Veteran's Affairs Philadelphia VA Regional Office and Insurance Center located at 5000 Wissahickon Ave, Philadelphia, PA, 19144 or call **1-800-669-8477.** Insurance Specialists available from 8:30 AM to 6:00 PM (Eastern Time), Monday - Friday; after hours/weekends messaging system is available. For more information – See http://www.vba.va.gov/ro/philly/contact.htm

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.

Individual wishing to obtain more information about access, redress and record correction of Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records should contact the Department of Veteran's Affairs Regional Office at **1-800-827-1000.** Veterans Services Representatives are available from 7:00 AM to 7:00 PM (Eastern Time), Monday thru Friday, except for federal holidays. For more information – see http://www.vba.va.gov/ro/philly/contact.htm

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 individuals whose records contain incorrect information may not receive notification of benefits/payments. Furthermore, incorrect information in IPS could result in letters sent to beneficiaries requesting incorrect payment.

Mitigation:
Insured individuals receive correspondence from the VA Insurance Payment system that will show the inaccurate information. All correspondence that is sent to the insured individuals contains POC information that can be utilized to contact the VA Insurance Payment system personnel to resolve issues. When an insured contact the VA Insurance Payment System personnel to discuss inaccurate data, at that time the data will be corrected within the system records. The insured individual will then receive updated correspondence which will show the updated accurate information.

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.

Per VA Directive and Handbook 6330, every 5 years the Office of Information Technology (OIT) develops, disseminates, and reviews/updates a formal, documented policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; along with formal, documented procedures to facilitate the implementation of the control policy and associated controls.

OIT documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and retains individual training records for 7 years. This documentation and monitoring are performed using Talent Management System (TMS).

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.

No, currently IPS has no contractors. OI&T provides basic security awareness training to all information system users (including managers, senior executives, and contractors) of VA information systems or VA sensitive information as part of initial training for new users, when required by system changes and annually thereafter.

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 which all personnel must complete via the VA's TMS. After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system.

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

If Yes, provide:

1. *The Security Plan Status,* Approved
2. *The Security Plan Status Date,* 03/30/2021
3. *The Authorization Status,* Authorization to Operate (ATO)
4. *The Authorization Date,*01/13/2021
5. *The Authorization Termination Date,* 01/13/2022
6. *The Risk Review Completion Date* 09/16/2020
7. *The FIPS 199 classification of the system* **(MODERATE).**

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.***

N/A

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, 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.

This question is related to privacy control UL-1, Information Sharing with Third Parties.

This is a mainframe system that does not use cloud technology.

9.2 Identify the cloud model being utilized.

Example: 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.

This is a mainframe system that does not use cloud technology.

9.3 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.
This is a mainframe system that does not use cloud technology.

9.4 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.

This is a mainframe system that does not use cloud technology.

9.5 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.

This is a mainframe system that does not use cloud technology.

9.6 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).

This is a mainframe system that does not use Robotics Process Automation (RPA) technology.

Section 9. 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: 2021.09.02 08:09:15 -04'00'

Privacy Officer, Rita Grewal

RICHARD S POWELL 116807

Digitally signed by RICHARD S POWELL 116807
Date: 2021.09.02 08:27:40 -04'00'

Information Security Systems Officer, Richard Powell

William J Wigton 247743

Digitally signed by William J Wigton 247743
Date: 2021.09.02 09:04:59 -04'00'

System Owner, William Wigton

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).

The System of Record Notice (SORN) "Veterans and Uniformed Services Personnel Programs of US Government Life Insurance – VA" 36VA29/83 FR 44407 dated 08/30/2018
This SORN can be found online at:

(https://www.oprm.va.gov/privacy/systems_of_records.aspx).

https://www.govinfo.gov/content/pkg/FR-2018-08-30/pdf/2018-18789.pdf