Privacy Impact Assessment for the VA IT System called:

Veteran Information/Eligibility Record Services

Veterans Benefits Administration (VBA)

Veteran Experience Office

Date PIA submitted for review:

09/28/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	*Cybil Mewborn*	*Cybil.Mewborn@va.gov*	*202-868-0489*
Information System Security Officer (ISSO)	*Eric Abraham*	*Eric.Abraham@va.gov*	*512-346-7422*
Information System Owner	*Fred Spence*	*Fred.Spence@va.gov*	*512-608-5331*

Abstract

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

The Veteran Information /Eligibility Record Services (VRS) platform provides data services, messaging, and DoD interoperability to Veterans Relationship Management (VRM) applications. It enables applications to search records and retrieve profile data, military history, and information on compensation and benefits, disabilities, and dependents. The system also provides a definitive, trusted, and consistent view of data to support fast, efficient, and consistent interaction with the veteran. It is a services tier and not exposed directly to users.

Overview

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

1 General Description

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

The Veteran Information/Eligibility Record Services (VRS) platform is owned by the Veterans Benefits Administration (VBA), Veteran Experience Services.

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

The Veteran Information /Eligibility Record Services (VRS) platform provides data services, messaging, and DoD interoperability to Veterans Relationship Management (VRM) applications. VRS system is enterprise middleware that resolves inconsistencies in data use, formats, and code sets from VA data repositories to the web-based applications. This allows those applications to search records and retrieve profile data, military history, and information on compensation and benefits, disabilities, and dependents, by creating a consistent view of the data. The data transferred includes PII, veteran military history, and veteran benefits information.

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

VA Owned and Operated, Veterans Benefits Administration (VBA), Veteran Experience Office

2. Information Collection and Sharing

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

VRS does not store information, it is a middleware "pipeline" that facilitates data transfer between VA internal applications. The data transferred numbers in the 100's of thousands for the typical veteran client.

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

The data transferred includes PII, veteran military history, and veteran benefits eligibility and utilization information, profile data, military history, and information on compensation and benefits, disabilities, and dependents.

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

The VRS is a portfolio of web services that are consumed by upstream systems. The VRS system acts as an enterprise middleware to interface with standard VA data repositories and downstream data services, thus abstracting the integration complexities from the consuming upstream systems. The portfolio of VRS services include: Digit to Digit (D2D) – Minor system under the VRS accreditation boundary; Affordable Care Act Service (ACA); One VA Pharmacy (1VAP); Enterprise Military Information Service (EMIS); Appeals Service; CP&E Adapter Services; VRS Military Information Service (VMIS) v1 and v2; and Business Event Notification Service (BENS). Information transferred includes individual profile data, military history, and information on compensation and benefits, disabilities, and dependents, by creating a consistent view of the data.

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

The VRS System is operated at only one site. The Austin Information Technology Center (AITC).

3. Legal Authority and SORN

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

The legal authority to include the Social Security Number (SSN) in the data transferred is used for identification of the veteran is Title 38, United States Code, Section 5106, and Title 38 United States Code 5701. 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. ”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." SORN is 138VA005Q - Veterans Affairs/Department of Defense Identity Repository (VADIR) - VA

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

The system is not in the process of being modified, and as such the SORN has not been modified. The system does not use cloud usage or storage.

D. System Changes

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

No. The completion of this PIA will not result in circumstances that changes to the current business processes.

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

No. The completion of this PIA could not potentially result in technological changes.

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 Information
- ☒ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers*
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☐ Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☒ Gender
- ☐ Integrated Control Number (ICN)

☒Military History/Service Connection
☒ Next of Kin
☒ Other Data Elements (list below)

- Competency, Incarcerated indicator
- Claim Folder Location, Regional Office of Jurisdiction (ROJ)
- Veteran Indicators/Flashes (eligibility or claims prioritization), Combat Veteran Indicator
- Income (Means Test, Veteran Eligibility Verification Report)
- Health Insurance (persons health and life insurance)
- Dependency/ Relationship (Relationship type, surrogacy, fiduciary, POA, NOK), information on those relations

Veteran military service history:
- Historical; VA Standard View of Basic Military History (eDD-214), LOD, Vietnam service, WWII service, Gulf War, OIF/OEF, etc.
- Current DoD Status
- VHA Enrollment Eligibility Supplemental Information
- CH33 Eligibility/Entitlement Supplemental Information
- Supplemental DoD Separation Pay/Retiree Pay Information

Veteran benefits information:
- Current Benefits Profile - summary of all benefits currently being received
- Current Veteran/beneficiary eligibility determinations
- Current Veteran Enrollment information
- Rating (Service connection, %, disability rating, SC, P&T, UI)
- Comp Award Status (award line - start, stop dates)
- Pension Award Status (award line - start, stop, dates)
- Payment History (Payments amount, recent payments, payment types, debt collections, copayments)
- Claim Information: Status of claims submitted (Disability Compensation, Pension, Education, etc.)
- Pending medical examination, examination results status, or other development items where a Veteran response is pending prior to promulgation of the decision
- Appeal Information: Status of appeals (claim for disability compensation or enrollment) pending and final decisions at the Board of Veterans Appeals
- Benefits eligibility profile (includes point in time Veteran "profiles" generated/stored periodically or produced on-demand, that outlines the VA benefits for which a given Veteran, service member or dependent may potentially be eligible)
- Veteran contact history: "The system shall support VA enterprise business process requirements for Contact History Information, inclusive of Claimant/Beneficiary comprehensive contact history information to support Self Service, Call Center, Walk Ins, Fulfillment (correspondence) and other Veteran contact business processes across all three administrations."

PII Mapping of Components (Servers/Database)

VRS consists of 3 key components (servers/databases/data services). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII used by Veteran Information/Eligibility Record Services components from internal application databases and the reasons for those databases collection of the PII are in the table below.

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

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Database 1	Yes	Yes	Veteran Name SSN Last Name First Name Middle Initial Gender Birthdate Final Notice Of Death Date Appellant: First Name Last Name	Facilitate identification of Veteran to obtain compensation benefits.	Encryption in transit; Encryption at rest
Database 2	Yes	Yes	SSN First Name Middle Name Last Name Date Of Birth Birth Date Txt Std Gender Id Death Date Gender Code	Facilitate identification of Veteran to obtain compensation benefits.	Encryption in transit; Encryption at rest

Database 3	Yes	Yes	Person Identifying Id First Name Middle Name Last Name	Facilitate identification of Veteran to obtain compensation benefits.	Encryption in transit; Encryption at rest

1.2 What are the sources of the information in the system?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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

The sources for the data are the Veterans Appeals Control and Locator System (VACOLS), the Administrative Data Repository (ADR), and the VA/DoD Identity Repository (VDR).

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

VRS provides data services, messaging, and DoD interoperability to Veterans Relationship Management (VRM) applications. It enables applications to search records and retrieve profile data, military history, and information on compensation and benefits, disabilities, and dependents from the VA data repositories.

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

VRS creates no information output.

1.3 How is the information collected?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

The VRM VIERS Appeals Service queries the Veterans Appeals Control and Locator System (VACOLS) database and retrieves electronically attached copies of Board of Veterans' Appeals decisions, remands and development memoranda; personal information on appellants and contesting parties including names, addresses, identifying numbers, phone numbers, service dates, and issues on appeal; names, addresses, and phone numbers of representatives, powers of attorney, and attorney fee agreements; information on and dates of procedural steps taken in claims; records of and copies of correspondence concerning appeals, diary entries, notations of mail received, and information requests; verbatim recordings and transcripts of hearings; tracking information as to file location and custodian; and employee productivity information. Information from ADR is sent via encrypted data transfer- mutual TLS. Information from VDR is sent via encrypted data transfer- mutual TLS (HTTPS).

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

VRS does not collect data. Data transported by VRS is derived from sources noted in 1.3 and 4.1.

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

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

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

- The VRS system assumes that information was checked for accuracy when it was first entered into the host system. All data is transmitted electronically within the VA network, or by using HTTPS. VRS has no mechanism for data checking.

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

The VRS System does not use data aggregation services.

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.

- Title 38, United States Code, Section 5106, and Title 38 United States Code 5701. 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." 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." Title 10 U.S.C. chapters 106a, 510, 1606 and 1607 and Title 38, U.S.C. Section 501(a) and Section 7304, Chapters 11, 13, 15, 18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51,53, and 55 provide the legal authority for operating the VRS system.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: There is a risk that Veteran data provided between systems may be incomplete.

Mitigation: Business rules within the VRS system ensure that data synchronization among the supported systems is successful. System administration personnel are alerted immediately when an error occurs.

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.

- Name - supports benefits, eligibility, identification and customer service.
- Social Security Number - supports benefits, eligibility, identification and customer service.
- Date of birth - supports benefits, eligibility, identification and customer service.
- Mailing Address - supports benefits, eligibility, identification and customer service.
- Zip code - supports benefits, eligibility, identification and customer service.
- Phone Number – supports customer service.
- Email address – supports customer service.
- Emergency Contact information (name, phone number, etc. of a different individual) – supports customer service.
- Financial Account Information - supports benefits, eligibility.
- Health Insurance beneficiary numbers account numbers - supports benefits, eligibility
- Race/ethnicity –supports VA Medical Statistical Analysis
- Veteran personal information: Demographics for Service members, Veterans, spouse/dependents (race, ethnicity, dob, DoD, gender) for detailed identification.
- Contact Information (mailing address, types of addresses, telephone numbers, email)- supports customer service, timely client notification.
- Financial Account (EFT preferences, Bank Address, other account information)- supports payment and claims.
- Competency, Incarcerated indicator - supports benefits, eligibility.
- Claim Folder Location, Regional Office of Jurisdiction (ROJ)- supports timely processing of requests.
- Veteran Indicators/Flashes (eligibility or claims prioritization) - supports benefits, eligibility.
- Combat Veteran Indicator - supports benefits, eligibility.
- Income (Means Test, Veteran Eligibility Verification Report) - supports benefits claims, eligibility.
- Health Insurance (persons health and life insurance) - supports benefits, eligibility.
- Dependency/ Relationship (Relationship type, surrogacy, fiduciary, POA, NOK), information on those relations – supports customer service, notification, benefits, eligibility.
- Veteran military service history: Historical; VA Standard View of Basic Military History (eDD-214), LOD, Vietnam service, WWII service, Gulf War, OIF/OEF, etc. - supports benefits, eligibility.
- Current DoD Status- supports benefits, eligibility.

- VHA Enrollment Eligibility Supplemental Information - supports benefits, eligibility.
- CH33 Eligibility/Entitlement Supplemental Information - supports benefits, eligibility.
- Supplemental DoD Separation Pay/Retiree Pay Information - supports benefits, eligibility, payments.
- Veteran benefits information: - supports benefits, eligibility.
- Current Benefits Profile - summary of all benefits currently being received - supports benefits, eligibility.
- Current Veteran/beneficiary eligibility determinations- supports benefits, eligibility.
- Current Veteran Enrollment information - supports benefits, eligibility.
- Rating (Service connection, %, disability rating, SC, P&T, UI) - supports benefits, eligibility.
- Comp Award Status (award line - start, stop dates) - supports benefits, eligibility.
- Pension Award Status (award line - start, stop, dates) - supports benefits, eligibility.
- Payment History (Payments amount, recent payments, payment types, debt collections, copayments) - supports benefits, eligibility, claims processing
- Claim Information: Status of claims submitted (Disability Compensation, Pension, Education, etc.) - supports benefits, eligibility, claims processing.
- Pending medical examination, examination results status, or other development items where a Veteran response is pending prior to promulgation of the decision - supports benefits, eligibility, claims processing.
- Appeal Information: Status of appeals (claim for disability compensation or enrollment) pending and final decisions at the Board of Veterans Appeals – supports veterans appeals processing.
- Benefits eligibility profile (includes point in time Veteran "profiles" generated/stored periodically or produced on-demand, that outlines the VA benefits for which a given Veteran, service member or dependent may potentially be eligible)VA – supports benefits, eligibility, claims processing
- Veteran contact history: "The system shall support VA enterprise business process requirements for Contact History Information, inclusive of Claimant/Beneficiary comprehensive contact history information to support Self Service, Call Center, Walk Ins, Fulfillment (correspondence) and other Veteran contact business processes across all three administrations." – supports timely customer service, identification, benefits, eligibility.

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

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

No data analysis occurs within VRS.

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

•

VRS does not create new information about any individual. VRS is a transport layer application that provides data to VA internal systems. Those other systems have their own processes/procedures for newly derived information use.

2.3 How is the information in the system secured?

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

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

•

- All data in transit uses Secure Socket Layers/Transport Layer Security (SSL/TLS), Simple Access Object Protocol (SOAP), or Java Database Connectivity (JDBC) over Hypertext Transfer Protocol (HTTPS). Data at rest is protected on the Storage Area Network (SAN) through ONTAP Internetwork Operating System (iOS), which is a fully FIPS 140-2, level 1 encryption compliant and meets the VA6500 requirements for data at rest encryption.

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

•

- All data in transit uses Secure Socket Layers/Transport Layer Security (SSL/TLS), Simple Access Object Protocol (SOAP), or Java Database Connectivity (JDBC) over Hypertext Transfer Protocol (HTTPS). Data at rest is protected on the Storage Area Network (SAN) through ONTAP Internetwork Operating System (iOS), which is a fully FIPS 140-2, level 1 encryption compliant and meets the VA6500 requirements for data at rest encryption.

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

- VA employees and contractors are required to take annual privacy training through the VA's Training Management System (TMS) and sign Rules of Behavior. Any employee or contractor who fails to recertify annually will have their VA network and application access suspended until they are in compliance with the requirement. VA employees and contractors are required to report all incidences of suspected or actual PII disclosure to a VA Information System Security Officer (ISSO) within one hour of discovering the incident. VA Handbook 6500.2, dated June 30, 2023, is the enterprise-wide Privacy Incident Response Plan. Privacy Service, OIT and Data Breach Response Service (DBRS) are responsible for implementation of VA Handbook 6500.2 as well as Privacy incident response plan procedures, including investigation and extra-agency reporting.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

2.4a How is access to the PII determined?

- All system administrators granted access to VA systems are given access based on their position, duties and a job related need to know. All system administrators are also required to have extensive training prior to receiving access and are required to recertify and resign the VA Rules of Behavior, annually, or lose their access to the VA network and applications until they are in compliance with the training requirements. System Administrator access is granted via the VA Electronic Permission Access System (ePAS).

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

- Supervisory approval for system administrators is documented in ePAS. Required Privacy and Security Training, which includes acceptance of responsibilities is documented in the VA Training Management System.

2.4c Does access require manager approval?

All system administrators granted access to VA systems are given access based on their position, duties and a job related need to know, and requires management approval. All system administrators are also required to have extensive training prior to receiving access and are required to recertify and resign the VA Rules of Behavior, annually. System Administrator access is granted via ePAS, and requires management approval.

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

- Administrative access and actions are logged in the VA's system and application log aggregation system, SPLUNK. Activity Reports may be run on an ad-hoc basis.

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

- VRS and VBA employ an Information System Security Officer (ISSO) whose primary duty is to monitor sensitivity levels assigned to VRS personnel, and to ensure appropriate security levels are assigned.

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*

- None of the information collected related to question 1.1 is retained by VRS.

3.2 How long is information retained?

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

VRS does not retain any information. It is a middleware application that provides "pipeline" sharing services between VA internal applications. Information retention is within each of the client applications and is relevant to each authorization boundary.

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

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

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

VRS does not retain any information. It has no database or method for retention.

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

VRS has no records retention schedule as VRS does not retain nor store any information.

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

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

VRS does not retain data nor is it directly accessed by any user. There are no records to eliminate.

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

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

VRS does not use PII for research, testing or training. Organizationally (VA), the use of PII during research, testing, and training is and it's reduced, when possible, to minimize risk. Risk minimization includes data obfuscation (use of partial PII), use of stale data, or use of anonymized data. Any use of data that may include PII must be documented and approved for use by VA leadership in accordance with VA Handbook 6502, VA Enterprise Privacy Program and VA Handbook 6508.1, Procedures for Privacy Threshold Analysis and Privacy Impact Assessment.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk: There is a risk that records could be modified during transfer.

Mitigation: VRS does not have an application tier that allows data manipulation. VRS provides a data integration service tier. All data is transmitted electronically within the VA network, or by using HTTPS.

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***
Administrative Data Repository (ADR)	Provides data for demographic, identity management, and eligibility/enrollment information for all persons who interact with the VAs Enrollment and Identity Services application.	• Sex • Personal Health Insurance Information (Insurance Coverage Dates) • Date of Death	JDBC connection

Veterans Benefits Administration Airborne Hazard Open Burn Pit Registry (AHOBPR)	Monitoring of the target population	• Current DoD Status
		  ○ Service Separation Date
		  ○ Retirement date
		  ○ Planned discharge data
			AHOBPR subscribes to an event queue published by VIERS

Veterans Benefits Administration Benefits Gateway Services (BGS)	VRS shares data information with BGS to support claims processing associated with D2D functionality. This information is	• Name • Date of Birth • Personal Mailing Address • Personal Phone Number • Personal Email Address • Social Security Number • Service Number	VIERS D2D pushes this information to various BGS/VBMS SOAP services via HTTPS

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*

	ultimately stored in the Corporate Data	• Sex (Gender)
		• Service Release Date(s)
		• Disability Information (Type, Date)
		• Disability Treatment History
		• Name History (ex: Maiden Name)
		• Military Branch of Service
		• Active Duty Status
		• Combat duty indicator
		• Enlistment Date
		• Discharge Date
		• National Guard Service Indicator
		• Inactive Pay Status
		• Future Payment Indicator
		• Retirement Payment Indicator
		• Pay amount
		• Direct Deposit Information (Bank name, account and routing number)
		• Insurance Number
		• Claimant Contact Information (address, phone, email)
		• Claimant Relationship Status
		• Veteran Indicators/Flashes
		  ○ Drug Abuse Indicator
		  ○ Alcohol Abuse Indicator
		  ○ HIV Indicator
			depending on which form is being processed

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*
		○ Sickle Cell Anemia Indicator ○ World War II Indicator ○ Post World War II Era Indicator ○ Korean Conflict Indicator ○ Post Korean Conflict Indicator ○ Vietnam Indicator ○ Post Vietnam Indicator ○ Gulf War Indicator ○ Operation Enduring Freedom Indicator ○ Operation Iraqi Freedom Indicator ○ Homeless Indicator • Employment History ○ Employer Name ○ Employer Location ○ Job description • Hospitalization Indicator • Hospital Address • Disability Rating • Income ○ Farm Operating Expenses ○ Primary Residence Acreage ○ Crop and Pasture Acreage ○ Signing Witness	

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*
		Name ○ Signing Witness Address ○ Rental Property Addresses ○ Rental Property Description ○ Business Valuation ○ Business Expenses ○ Business Income ○ Social Security Income ○ US Civil Service Income ○ US Railroad Retirement Income ○ Black Lung benefits Income ○ Service Retirement Income • Dependency/Relationship Information ○ Marital History ○ Spouse Social Security Number ○ Dependent Names ○ Dependent Birthdays ○ Dependent Addresses ○ Child SSN ○ Child Data of Birth ○ Child Name	

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*
		○ Child Tuition Details ○ Child Income ○ Child Savings	
Veterans Benefits Administration Data Access Services (DAS)	Provides data for multiple systems supporting Veteran and Service Member medical, benefit, personnel and personal/administrative information.	• SSN • Insurance Enrollment Periods / Status	DAS/VLER interacts with the VIERS ACA Soap Services as well as D2D form submission SOAP services.
Office of Information and Technology Digital-Transformation-Center Integration Platform (DIP)	Provides data for multiple systems supporting Veteran and Service Member combat and service indicators, medical, benefit, personnel and personal/administrative information.	• Combat Pay Indicator • Combat Pay Dates • Name • SSN • Date of Birth • Address • Nearest Relative Name • Nearest Relative Address • • Service Dates • Veteran Indicators/Flashes ○ Foreign Service Indicator ○ Sea Service Indicator ○ Combat Pay Indicator ○ Reentry Indicator ○ Post 911 Deployment Indicator	DIP Requests information from VIERS SOAP services via HTTPS

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*
		○ Post 911 Combat Indicator ○ Pre 911 Deployment Indicator ○ Active Duty Indicator • Sex (Gender) • Date of Death • Rating ○ Disability Rating ○ Disability Percent ○ Disability Permanence Indicator ○ Disability Pay ○ Disability Date	
Veterans Benefits Administration Enrollment System (ESR)	Veteran Eligibility and enrollment information	• Current DoD Status ○ Service Separation Date ○ Retirement date ○ Planned discharge data	ESR subscribes to an event queue published by VIERS
Veterans Experience Office Enterprise Veterans Self Service (EVSS)	Veteran Eligibility and enrollment information	• Name • Service Branch • SSN • Date of Birth • Sex (Gender) • Date of Death • Address • Dependency/Relationship ○ Nearest Relative Name ○ Nearest Relative Address • Veteran	EVSS requests data from VIERS through SOAP services via HTTPS

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*
		Indicators/Flashes ○ Foreign Service Indicator ○ Sea Service Indicator ○ Reentry Indicator ○ Reserve Indicator ○ Post 911 Deployment Indicator ○ Post 911 Combat Indicator ○ Pre 911 Deployment Indicator ○ Active Duty Indicator • Rating ○ Disability Rating ○ Disability Percent ○ Disability Permanence Indicator ○ Disability Pay ○ Disability Date ○ Insurance Enrollment Periods / Status	
Veterans Benefits Administration IAM - Master Person Index	Consolidated VA end-user validation and authorization	• Service Separation Date • Retirement date • Planned discharge data • Title 38 Status	IAM/MPI subscribes to an event queue published by VIERS
Veterans Benefits Administration Loan Guaranty Service (LGY)	Verify veteran identity	• Service Episode Dates • Service Episode Termination Reasons	LGY requests this data from VIERS

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*
		• Retirement Types • Discharge Status • Reason for Separation • Pay Grade • Service Rank • Service Entry Dates • Reserve Status	via the VIERS SOAP services
Office of Information Technology Lighthouse		• Time spent in Specialty • Service Dates • Foreign Service Indicator • Sea Service Indicator • Pay Grade • Decoration/Awards Records • Military Education History • ROTC Indicator • Load Repayment Indicator • Leave Duration • Dental Service Indicator • Address • Nearest Relative Name • Nearest Relative Address • Separation Reason • Reentry Indicator • Deployment History • Reserve Indicator • Reserve Drill Day Information • Title 38 Status • Post 911 Deployment Indicator • Post 911 Combat Indicator • Pre 911 Deployment Indicator	Requests from Lighthouse to VIERS services are SOAP via HTTPS Requests from VIERS to Lighthouse are REST via HTTPS

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*
		• Active Duty Indicator • Sex • Race • Ethnicity • Education Level Indicator • Date of Death • Disability Rating • Disability Percent • Disability Permanence Indicator • Disability Pay • Disability Date • Service Occupation • Service Occupation Dates • Insurance Enrollment Periods / Status	
Veterans Experience Office Veteran-facing Services Platform (VA.gov)		• Time spent in Specialty • Service Dates • Foreign Service Indicator • Sea Service Indicator • Pay Grade • Decoration/Awards Records • Military Education History • ROTC Indicator • Load Repayment Indicator • Leave Duration • Dental Service Indicator • Address • Nearest Relative Name • Nearest Relative Address • Separation Reason • Reentry Indicator • Deployment History	SOAP service via HTTPS or through a direct database connection over JDBC

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*
		• Reserve Indicator • Reserve Drill Day Information • Title 38 Status • Post 911 Deployment Indicator • Post 911 Combat Indicator • Pre 911 Deployment Indicator • Active Duty Indicator • Sex • Race • Ethnicity • Education Level Indicator • Date of Death • Disability Rating • Disability Percent • Disability Permanence Indicator • Disability Pay • Disability Date • Service Occupation • Service Occupation Dates	
Veterans Benefits Administration Veterans Experience Integration Solution (VEIS)	Data retrieval	• Appeal Status • Appeal Docket Number • Appeal History • Appeal Dates • Appeal Decision • Appeal Medical Facility • Insurance Infomation • Appellant Address • Appellant Name • Payment History • SSN	VEIS calls VIERS SOAP services via HTTPS

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*
		• IEN • Account Amount Owed • Account Amount Paid • Debtor Address • Debtor Name • Debtor FMS Name • Date of Birth • Beneficiary Sponsor SSN • Beneficiary Sponsor Name • Beneficiary Sponsor Sex • Beneficiary Sponsor Address • Beneficiary Sponsor ChampVA Indicator • Beneficiary Sponsor ChampVA status • Beneficiary Sponsor Spina Bifida Indicator • Beneficiary Sponsor Form 3884 Date/Indicator • Beneficiary Relationship to Sponsor • Beneficiary SSN • Beneficiary Name • Beneficiary Address • Beneficiary Sex • Beneficiary Date of Death • Beneficiary Phone Number • Beneficiary ChampVA Indicator • Beneficiary ChampVA Status • Beneficiary Spina Bifida Indicator • Beneficiary Deductible	

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*
		• Beneficiary Cap • Beneficiary Restriction Information • Communication History • Claim History • Claim amounts • Claim Status • Claim Provider • Claim Date • Claim Rejection Reasons • Claim Comments • Claim Payment Method • Claim Data • Medication Details • Medicare Eligibility Data • Tricare Indicator • Physician Name • Foreign Medication Provider Payments • Foreign Medication Provider Check and Bill information • Mental Health Visit Allowance • Medical Provider NPI • Medical Provider Type • Medical Provider Billing Information • Medical Provider • Time spent in Specialty • Service Dates • Foreign Service Indicator • Sea Service Indicator • Pay Grade • Decoration/Awards Records • Military Education History	

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*
		• ROTC Indicator • Load Repayment Indicator • Leave Duration • Dental Service Indicator • Address • Nearest Relative Name • Nearest Relative Address • Separation Reason • Reentry Indicator • Deployment History • Reserve Indicator • Reserve Drill Day Information • Title 38 Status • Post 911 Deployment Indicator • Post 911 Combat Indicator • Pre 911 Deployment Indicator • Active Duty Indicator • Sex • Race • Ethnicity • Education Level Indicator • Date of Death • Disability Rating • Disability Percent • Disability Permanence Indicator • Disability Pay • Disability Date • Service Occupation • Service Occupation Dates	

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 VA/DoD Identity Repository (VDR)	Provides data for data transfers between the VA Business Lines and DoD	• Veteran Name • POW Periods • Mental Health Episode Periods	Depending on the service used this might be VIERS to VDR through a SOAP service via HTTPS or through a direct database connection over JDBC
Veterans Benefits Administration Veterans Online Application - Direct Connect (VDC) (My eBenefits Web Portal) (EBN)	VRS transfers data to VDC for Analysis and Statistics	• Name • Date of Birth • Personal Mailing Address • Personal Phone Number • Personal Email Address • Social Security Number • Service Number • Sex • Service Release Date(s) • Homeless Indicator • POC Phone Number • Disability Information (Type, Date) • Disability Treatment History • Name History (ex: Maiden Name) • Military Branch of Service • Active Duty Status • Combat duty indicator • Enlistment Date • Discharge Date • National Guard Service	SOAP service via HTTPS or through a direct database connection over JDBC

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*
		Indicator • Inactive Pay Status • Future Payment Indicator • Retirement Payment Indicator • Pay amount • Direct Deposit Information (Bank name, account and routing number) • Power of Attorney name • Insurance Number • Claimant Contact Information (address, phone, email) • Claimant Relationship Status • VA Representative Name and employment details • Drug Abuse Indicator • Alcohol Abuse Indicator • HIV Indicator • Sickle Cell Anemia Indicator • Years of Education • Vocational Rehabilitation History • Employer Name • Employer Location • Job description • Hospitalization Indicator • Hospital Address • Disability Rating • World War II Indicator • Post World War II Era Indicator • Korean Conflict Indicator	

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*
		• Post Korean Conflict Indicator • Vietnam Indicator • Post Vietnam Indicator • Gulf War Indicator • Operation Enduring Freedom Indicator • Operation Iraqi Freedom Indicator • Gross Farming related Receipts • Farm Earnings History • Information pertaining to the names and identifiers of any owned businesses • Farm Operating Expenses • Primary Residence Acreage • Crop and Pasture Acreage • Signing Witness Name • Signing Witness Address • Rental Property Addresses • Rental Property Description • Business Valuation • Business Expenses • Business Income • Marital History • Spouse Social Security Number • Dependent Names • Dependent Birthdays • Dependent Addresses • Social Security Income	

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*
		• US Civil Service Income • US Railroad Retirement Income • Black Lung benefits Income • Service Retirement Income • Child SSN • Child Data of Birth • Child Name • Child Tuition Details • Child Income • Child Savings • Service Decorations • Combat Indicator • Service Rank • Separation Reason • Active Duty End Date • Character of Service • Period of Service start date(s) • POW Indicator • POW Country • POW Dates • Service Episode Date(s) • Service Episode Termination Reason(s) • Discharge character of service • Personnel Organization Code • Personnel Category • Retirement Type • Training Date • Initial Entry Date • Deployment History • Guard Status	

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*
		• Military Occupation • Unit Service History • Pay History	
Veterans Benefits Administration Veterans Appeals Control and Locator System (VACOLS)	Status of appeals (claim for disability compensation or enrollment) pending and final decisions at the Board of Veterans Appeals	• Claimant Contact Information (address, phone, email) • Claimant Relationship Status • Appeal Status • Appeal Docket Number • Appeal History • Appeal Dates • Appeal Decision • Appeal Medical Facility • Insurance Information	SOAP service via HTTPS or through a direct database connection over JDBC
Veterans Benefits Administration Claims Processing & Eligibility System (CP&E)	Supports benefits, eligibility, identification and customer service	• Claimant Contact Information (address, phone, email) • Claim Number • Claim Status	SOAP service via HTTPS or through a direct database connection over JDBC

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: Inadvertent data disclosure or a data breech could occur from systems using VRS to transfer data.

Mitigation: All system-to-system connections are encrypted to further prevent unauthorized access to Veteran data during transmission (Reference Question 4.1, Column 4). VA users with access to sensitive data or VA information systems must read and acknowledge the rules of behavior (ROB) prior to gaining access and annually thereafter. The ROB provides details for data protection, use and handling.

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	***List the purpose of information being***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding***	***List the method of transmission and the***

shared/received with	***shared / received / transmitted with the specified program office or IT system***		***agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***measures in place to secure data***
N/A	N/A	N/A	N/A	N/A

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, VRS has no external connections.

Mitigation: Not Applicable, VRS has no external connections.

Section 6. Notice

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

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

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

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

The VRS system provides no notices to individuals, as VRS shares no data and has no user interface. Source systems for the data collected or processed described in section 4.1 and 5.1 are responsible to notify.

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

Please provide response here

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

The VRS system provides no notices to individuals, as VRS shares no data and has no user interface. Source systems for the data collected or processed described in section 4.1 and 5.1 are responsible to notify.

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.

Any opportunity to decline providing information occurs prior to the VRS processes. VRS receives all data from other information 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.

Veterans do not have the right to consent to any data used by the VRS system. Any opportunity to provide consent would be during the collection process of the upstream source systems supplying data to VRS.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.
Follow the format below:

Privacy Risk: Inadvertent data disclosure or a data breach could occur from upstream systems using VRS to transfer data and those upsteam data sources not having appropriately notified individuals of collection of PII.

Mitigation: The VRS system provides no notice to individuals, as VRS shares no data and has no user interface. Source systems for the data collected or processed described in section 4.1 and 5.1 are responsible to notify end users of the purpose for which the information is collected, and communicating the procedures in place to ensure that the data is used only for the purpose articulated in the 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?

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

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web***

page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.

The VRS system does not have an application tier, or user interface. Procedures for individuals to gain access to their information would be based upon procedures for those data sources.

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

The VRS system does not have an application tier, or user interface. Procedures for individuals to gain access to their information would be based upon procedures for those data sources.

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

The VRS system does not have an application tier, or user interface. Procedures for individuals to gain access to their information would be based upon procedures for those data sources, not VRS.

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.

The VRS system does not have an application tier to add, change, or delete data; instead, it provides a data integration service tier to other applications. Procedures for individuals to gain access to their information for correcting inaccuracies would be based upon procedures for those data sources.

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.

Procedures for individuals to correct their information would be based upon procedures for the data sources.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Details involving redress for data held in any of the host databases are addressed in that system's respective Privacy Impact Assessment. PIAs are located at http://www.oprm.va.gov/privacy/ to find the specific PIA, and http://www.oprm.va.gov/privacy /privacy-act-requests/ to gain access to their specific records 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.*** *(Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

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

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?
This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk: Inadvertent data disclosure or a data breach could occur from upstream systems using VRS to transfer data and those upstream data sources not having appropriately notified individuals of procedures associated with access to, preventing the use of, or the correction of any PII data collected by said system.

Mitigation: VRS does not retain, edit, or delete information, thus, the VRS system provides no notice to individuals, as VRS shares no data and has no user interface. Source systems for the data collected or processed described in section 4.1 and 5.1 are responsible to notify end users of the procedures for which the end user may request whether information is collected about them;

what procedures the end user may follow to correct any information that may be collected about them; and, procedures to prevent personal information about a user collected for one purpose being used for another purpose not communicated to the user. These procedures would be published in privacy or public notices associated with each upstream system actually doing the data collection.

Section 8. Technical Access and Security

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

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

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

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

There is no user interface to VRS; only system administrators have access to the server hardware and operating system. Administrators undergo a background investigation, their access is documented and verified through the MyVA Elevated Privileges Request in ePAS, and they must agree to additional rules of behavior for system administration personnel.

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

No users from other agencies have access to VRS.

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

Only system administrators have access to the server hardware and operating system. VRS has no data user interface and no data users.

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.

Contractors may have access to VRS infrastructure. All contractors sign the VA Rules of Behavior, just as VA Employees do, and they pass a Background Investigation prior to receiving access to PayVA.VA contract employee access is verified through the Contracting Officer's Representative (COR) and other VA supervisory/administrative personnel before access is granted to any VA system. Contractor access is reviewed annually at a minimum. 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 Talent Management System (TMS). All contractors are vetted using the VA background investigation process and must obtain the appropriate level background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access. Generally, contracts are reviewed at the start of the initiation phase of acquisitions and again during procurement of option years by the Contracting Officer, Information Security Officer, Privacy Officer, COR, Procurement Requestor/Program Manager and any other stakeholders required for approval of the acquisition. Contracts generally have an average duration of 1-3 years and may have option years stipulated in the original contract.

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 VA Privacy and Security Awareness training which all personnel must complete via the VA's Talent Management System (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 retained via electronic acknowledgment and is tracked through the TMS system. 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. System administrators are required to complete additional role-based training.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 06/30/2022
3. *The Authorization Status:* Authority to Operate (ATO)
4. *The Authorization Date:* 02/08/2021
5. *The Authorization Termination Date:* 01/26/2024
6. *The Risk Review Completion Date:* 09/05/2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* High

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

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

N/A

Section 9 – Technology Usage

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

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

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

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

The system does not use Cloud technology.

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

The system does not use Cloud technology.

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.

The system does not use Cloud technology.

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.

The system does not use Cloud technology.

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).

The system does not use RPA technology.

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 they provided in this Privacy Impact Assessment is true and accurate.

CYBIL MEWBORN

Digitally signed by CYBIL MEWBORN
Date: 2023.11.13 08:16:18 -05'00'

Privacy Officer, Cybil Mewborn

Eric Abraham 3564094

Digitally signed by Eric Abraham 3564094
Date: 2023.10.30 08:03:21 -05'00'

Information System Security Officer, Eric Abraham

FRED SPENCE

Digitally signed by FRED SPENCE
Date: 2023.10.27 09:23:21 -05'00'

Information System Owner, Fred Spence

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy, a Privacy Act notice on forms).

This is not applicable to VRS System. The system has no users nor user interface. Data cannot be accessed directly from VRS.

HELPFUL LINKS:

Record Control Schedules:

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

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

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

National Archives (Federal Records Management):

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

VHA Publications:

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

VA Privacy Service Privacy Hub:

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

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices