Privacy Impact Assessment for the VA IT System called:

VA DoD Identity Repository - Amazon Web Services

VACO

Veterans Relationship Management (VRM)

Date PIA submitted for review:

03-16-2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Julie Drake	Julie.drake@va.gov	202-632-8431
Information System Security Officer (ISSO)	Abraham Eric	Eric.Abraham@va.gov	512-987-7731
Information System Owner	Torres Alexander	alexander.torres@va.gov	703-300-5511

Abstract

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

The Veterans Affairs/Department of Defense Identity Repository-Amazon Web Services (VDR-AWS) database is an electronic repository of military personnel's military history, payroll information and their dependents' data provided to VA by the Department of Defense's Defense Manpower Data Center (DMDC) using the Defense Enrollment Eligibility Reporting System (DEERS). The Department of Defense is the owner of the data within VDR-AWS. The VDR-AWS is simply storing this information provided by the DoD and using it to provide an electronic consolidated view of comprehensive eligibility and benefits utilization data from across VA and DoD. The VDR-AWS database repository is used in conjunction with other applications across VA business lines to provide an electronic consolidated view of comprehensive eligibility and benefits utilization data from across VA and DoD. VA applications use the VDR-AWS database to retrieve profile data, as well as address, military history, and information on compensation and benefits, disabilities, and dependents.

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.

VA DoD Identity Repository - Amazon Web Services and the Program Office that owns the system is Veterans Relationship Management (VRM)

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

The VDR-AWS is simply storing this information provided by the DoD and using it to provide an electronic consolidated view of comprehensive eligibility and benefits utilization data from across VA and DoD. The VDR-AWS database repository is used in conjunction with other applications across VA business lines to provide an electronic consolidated view of comprehensive eligibility and benefits utilization data from across VA and DoD. VA applications use the VDR-AWS database to retrieve profile data, as well as address, military history, and information on compensation and benefits, disabilities, and dependents.

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

VDR-AWS system is owned by the Veterans Relationship Management (VRM) program and maintained by IT Operations (ITOPS), Service Operations, Infrastructure Operations (IO), Platform Support.

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.

VDR-AWS stores information on approximately 27 million Veterans.

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

The VDR-AWS is simply storing this information provided by the DoD and using it to provide an electronic consolidated view of comprehensive eligibility and benefits utilization data from across VA and DoD. The VDR-AWS database repository is used in conjunction with other applications across VA business lines to provide an electronic consolidated view of comprehensive eligibility and benefits utilization data from across VA and DoD. VA applications use the VDR-AWS database to retrieve profile data, as well as address, 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 Veterans Affairs (VA) Department of Defense (DoD) Identity Repository-Amazon Web Services (VDR-AWS) system is owned by the Veterans Relationship Management (VRM) program and maintained by IT Operations (ITOPS), Service Operations, Infrastructure Operations (IO), Platform Support.

VDR-AWS is a unified collection and distribution point for data transfers between the various VA business systems and the DoD. The Department of Defense is the owner of all of the data within VDR-AWS. The VDR-AWS is simply storing this information provided by the DoD and using it to provide an electronic consolidated view of comprehensive eligibility and benefits utilization data from across VA and DoD. VDR-AWS stores information on approximately 27 million Veterans.

DoD owns the data and has exclusive disposition and retention of all data records.
VDR-AWS data is a subset of the DoD, Defense Manpower Data Center (DMDC), Personnel Database. DoD replicates the data to the VA. The VA's copy is read only and as such the VA does not add records to the database, update data or delete data. DoD DMDC has sole responsibility for the management of the data. VA only reads the data.

VDR-AWS receives information from two sources external to the VA, and one internal to the VA. The first external source is from the DoD's Defense Enrollment Eligibility Reporting System (DEERS) database and consists of the Veteran's non-medical service information. The second external source is with Prudential Life Insurance, which provides tracking and benefit details of the Veteran's Servicemen's Group Life Insurance (SGLI) and transition to Veterans' Group Life Insurance (VGLI). The internal source is with the Stakeholder's Enterprise Portal, which maintains a Veteran's demographic information.

VDR-AWS provides all the information it stores to multiple systems. The primary user interface is through the Veterans Information Solution (VIS), which is simply a view-only front-end user interface for authorized VA employees to the data stored within the VDR-AWS database. The Veteran Information/Eligibility Records Services (VRS) system, which is used to store data used in processing benefits eligibility and is used by other Veteran Relationship Management (VRM) applications. Other connections exist to the VA Customer Relationship Management/Unified Desktop (CRM/UD), VA Federal Case Management Tool (FCMT), and Stakeholder Enterprise Portal (SEP), which are used for correlation of Veteran demographic data. VDR-AWS shares DD-214 information received from DoD with Beneficiary Identification and Locator System (BIRLS) for permanent storage of the digital

DD-214 document. It also sends VA education and benefits payment information back to DEERS to update the DoD payment and education database systems.

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 Version Date: October 1, 2017 Page 3 of 27 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. Completion of this PIA will not result in technology changes, or changes to the SORN Defense Enrollment Eligibility Reporting Systems (DEERS), DMDC 02 DoD (October 16, 2019, 84 FR 55293; corrected December 2, 2019, 84 FR 65975). DMDC-02-DoD.pdf (defense.gov). VDR-AWS does not use cloud technology.

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.

VDR-AWS receives PII data by data replication from DEERS and has no contact with subjects. Data is received from Prudential Life Insurance via secure data transfer. Data is received from Stakeholder's Enterprise Portal via an encrypted data connection.

3. Legal Authority and SORN

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

Benefits and Services for Members being Separated or Recently Separated; 10 U.S.C. Chapter 75, Deceased Personnel; 10 U.S.C 2358 and Miscellaneous Rights and Benefits; 10 U.S.C. Chapter 54.

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 current SORN in place is SORN Defense Enrollment Eligibility Reporting Systems (DEERS), DMDC 02 DoD (October 16, 2019, 84 FR 55293: corrected December 2, 2019, 84 FR 65975). DMDC-02-DoD.pdf (defense.gov)

D. System Changes

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

No.

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

No.

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)

Additional Elements:

Alias, Benefit information, education benefit participation, eligibility and usage, healthcare benefit periods of eligibility (TRICARE, CHAMPVA), alias.

PII Mapping of Components (Servers/Database)

VA DoD Identity Repository - Amazon Web Services consists of one key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by VA DoD Identity Repository - Amazon Web Services and the reasons for the collection of the PII are in the table below.

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

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Veterans Administration / Department of Defense Identity Repository VADIR (Instances): VDR-AWS-PROD, VDR-AWS-PREPROD	Yes	Yes	Name • Social Security Number • Date of Birth • 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 •Race/Ethnicity • Tax Identification Number • Gender • Military History/Service Connection • Alias • Benefit information • Education benefit participation, eligibility, and usage • Healthcare benefit periods of eligibility (TRICARE, CHAMPVA)	To identify retired veterans and dependent members of their families who have entitlement to DoD benefits but who are not identified in the DEERS program and to assist in determining eligibility for Civilian Health and Medical Program of the Uniformed Services (CHAMPUS) benefits	Data transfer and at rest is FIPS 2.0 encrypted. The security for data at rest is Oracle Database Security 19c and in transit is using VA approved transfer methods (e.g.: SFTP, one drive, Teams, HTTPS with TLS, etc.)

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?

VDR-AWS receives data from the following: Defense Enrollment/Eligibility Reporting System (DEERS), Prudential Life Insurance and Stakeholder's Enterprise Portal

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.

VDR-AWS receives information from two sources external to the VA, and one internal to the VA. The first external source is from the DoD's Defense Enrollment Eligibility Reporting System (DEERS) database and consists of the Veteran's non-medical service information. The second external source is with Prudential Life Insurance, which provides tracking and benefit details of the Veteran's Servicemen's Group Life Insurance (SGLI) and transition to Veterans' Group Life Insurance (VGLI). The internal source is with the Stakeholder's Enterprise Portal, which maintains a Veteran's demographic information.

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

DoD owns the data and has exclusive disposition and retention of all data records. VDR-AWS data is a subset of the DoD, Defense Manpower Data Center (DMDC), Personnel Database. DoD replicates the data to the VA. The VA's copy is read only and as such the VA does not add records to the database, update data or delete data. DoD DMDC has sole responsibility for the management of the data. VA only reads the data

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?

VDR-AWS receives PII data by data replication from DEERS and has no contact with subjects. Data is received from Prudential Life Insurance via secure data transfer. Data is received from Stakeholder's Enterprise Portal via an encrypted data connection.

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.

VDR-AWS does not collect data using a form.

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.

VDR-AWS information was checked for accuracy when it was first entered into the host system from which the data is received. As a storage system, it has no logic for error-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.

VDR-AWS information was checked for accuracy when it was first entered into the host system from which the data is received. As a storage system, it has no logic for error-checking.

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

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (*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: Because VDR-AWS collects its data from external sources, there is a risk that data could be corrupted during data transfer and/or host system data entry.

Mitigation: VDR-AWS uses a Cyclic Redundancy Check (CRC) to ensure that the data it receives matches exactly what is sent. The CRC number is passed with the data, and the VDR-AWS database ensures that it receives the same number when it makes its own calculation. If it does not, the system will request retransmission from the sending system. The host system operator follows local procedures to ensure that the data being entered is correct prior to committing it to the host database

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: Confirm veteran's identification, internal and external
Social Security Number: Confirm veteran's identity, create file number for veteran, confirm Social Security Administration benefits, internal and external
Date of Birth: used to verify Veteran identity
Mailing Address: Used to correspond with the Veteran
Phone Number: Used to correspond with the Veteran
Fax Number: Used to correspond with the Veteran
Email Address: Used to correspond with the Veteran

Race/Ethnicity: Assists in uniquely identifying the person's record.
Maiden Name: Assists in uniquely identifying the person's record.
Alias: Assists in uniquely identifying the person's record.
Family Relations: Assists in uniquely identifying the person's record.
Service Information: Assists in uniquely identifying the person's record.
Education: Assists in uniquely identifying the person's record.
Benefit Information: Assists in uniquely identifying the person's record.
Association to dependents: Assists in uniquely identifying the person's record.
Military Service Participation: Assists in uniquely identifying the person's record.
Reason and nature of active-duty separation: Assists in uniquely identifying the person's record.
Combat/environmental exposures: Assists in uniquely identifying the person's record.
Guard/Reserve activations: Assists in uniquely identifying the person's record.
Military casualty/disabilities: Assists in uniquely identifying the person's record.
Education benefit participation: Assists in uniquely identifying the person's record.
Eligibility and usage: Assist in uniquely identifying the person's record.
Healthcare benefit periods of eligibility: Assists in uniquely identifying the person's record.
VA Compensation: Assists in uniquely identifying the person's record.

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 the VDR-AWS system. It merely provides stored data to other data analysis and access systems.

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.

No data analysis occurs within the VDR-AWS system. It merely provides stored data to other data analysis and access systems.

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 files shared by VDR-AWS are sent via Secure File Transfer Protocol (SFTP). Web services pull SSNs via Secure Socket Layer (SSL) links internal to the VA Network.

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

All files shared by VDR-AWS are sent via Secure File Transfer Protocol (SFTP). Web services pull SSNs via Secure Socket Layer (SSL) links internal to the VA Network.

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

The system uses secure transmission for data transfers. Encryption techniques also utilized include SOAP via HTTPS Web Services, Oracle SQL*NET advanced encryption, site to site VPN, SFTP. At rest, the data is behind the multiple layers of security afforded to it by the internal VA network plus the standard security provided with ORACLE 19c, configured in accordance with VA standards. There are no additional protections in place.

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?

VA employees/contractors use ePASS and require approvals from supervisors. OIT technology connections are processed through ServiceNow and approved by the Information system owner. Ad-hoc reports are also approved by the Information system owner.

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

Yes, it is documented in the VDR-AWS SharePoint Site – VADIR confluence site.

2.4c Does access require manager approval?

Yes, access's require supervisor/ISO approvals.

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

Attachmate Reflection is terminal emulator session software used for command line access by authorized system administrators. There is no automated reporting or user interface; reports are generated directly from the database by authorized administrators only. Please see the Veterans

Information Solution (VIS), Beneficiary Identification and Records Locator (BIRLS), Veteran Information/Eligibility Records Services (VRS), VA Customer Relationship Management/Unified Desktop (CRM/UD), VA Federal Case Management Tool (FCMT), and Stakeholder Enterprise Portal (SEP) PIAs for details on end-user privacy controls. http://www.oprm.va.gov/privacy/pia.aspx

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

Authorized system administrators.

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.*

The following information is collected and retained on the VDR-AWS system: Name, Social Security Number, Date of Birth, Personal Mailing Address, Personal Phone Numbers, Personal Fax numbers, Personal Email, Emergency Contact Information (Name, Phone Number, etc. of a different individual), Financial Information, Race/Ethnicity, Tax Identification Number, Gender, Military History/Service Connection, Alias, Benefit information, Education benefit participation, eligibility, and usage, Healthcare benefit periods of eligibility (TRICARE, CHAMPVA).

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.*

As a storage system reflecting the current state of the host system at DMDC, VADIR reflects the contents of that host system. It is, therefore, up to that system to create or dispose of records in accordance with their data retention policy.

The Veteran's record is to be destroyed upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later. Guidelines stated in General Records Schedule (GRS) 5.2, item 020 DAA-GRS-2017-0003-0001. grs05-2.pdf (archives.gov).

Final document repository/official records are stored and maintained in the receiving system listed on the internal sharing table. This system is a pass through and not record repository.

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.
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?

Yes. These records are retained in accordance with the General Records Schedule Section 5.2 GENERAL RECORDS SCHEDULE 5.2: Transitory and Intermediary Records, approved by National Archives and Records Administration (NARA). http://www.archives.gov/records-mgmt/grs.html

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

These records are retained in accordance with the General Records Schedule Section 5.2 GENERAL RECORDS SCHEDULE 5.2: Transitory and Intermediary Records, approved by National Archives and Records Administration (NARA). http://www.archives.gov/records-mgmt/grs.html

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.

It is VA policy that all Federal records contained on paper, electronic, or other medium are properly managed from their creation through their final disposition, in accordance with Federal laws, the General Records Schedule (GRS).
Electronic records are disposed of in accordance with the OIT-OIS SOP MP-6-Electronic Media Sanitization policy.
Paper records are disposed of in accordance with the OIT VA Directive 6371-Destruction of Temporary Paper Records.

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.

VDR-AWS does not use PII for training or testing but does for research.
VA Directive 6502 (page 1) sets policy to limit data access to PII to only individuals with a need for that information in order to perform their official duties; and to minimize the collection and maintenance of data to that necessary to perform the official functions of the Department. Further, VHA Directive 1200.01 (page 5) and VHA Directive 1605.01 (page 38) define the policy that minimizes the use of PII for research. Primary Conditions for access to PII for research purposes involves approval by an Institutional Review Board or Privacy Board, Preparatory to research.

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 the information maintained by VDR-AWS could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation: To mitigate the risk posed by information retention, it is VA policy that all Federal records contained on paper, electronic, or other medium are properly managed from their creation through their final disposition, in accordance with Federal laws, the General Records Schedule (GRS). Electronic records are disposed of in accordance with the OIT-OIS SOP MP-6-Electronic Media Sanitization policy. Paper records are disposed of in accordance with the OIT VA Directive 6371-Destruction of Temporary Paper Records.

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***
Digital GI Bill	The interface is to provide the Benefits Delivery Network (BDN) with a monthly file of military service information used for education eligibility and to calculate education award payment amounts. It	• Name • Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number • Personal Email Address • Emergency Contact Information (Name, Phone	Encrypted Data Connection Internal to the VA

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*
	different from the Chapter 30 extract, as Chapter 1606 is for Selected Reserve only.	Number, etc. of a different individual) • Financial Information • Race/Ethnicity • Tax Identification Number • Gender • Military History/Service Connection • Alias • Benefit information • Education benefit participation, eligibility, and usage • Healthcare benefit periods of eligibility (TRICARE, CHAMPVA)	
VA Profile	Correlation of demographic data	• Name • Social Security Number • Date of Birth • 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 • Race/Ethnicity • Tax Identification Number • Gender • Military History/Service Connection • Alias • Benefit information • Education benefit participation, eligibility, and usage • Healthcare benefit periods of eligibility (TRICARE, CHAMPVA)	Encrypted Data Connection Internal to the VA

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 Tracking Application	Veteran Identity & Mil History	• Name • Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number0 Personal Email Address • Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Financial Information • Race/Ethnicity • Tax Identification Number • Gender • Military History/Service Connection	Encrypted Data Connection Internal to the VA
Federal Case Management Tool	Veteran Identity & Mil History	• Name • Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number0 Personal Email Address • Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Financial Information • Race/Ethnicity • Tax Identification Number • Gender • Military History/Service Connection	Encrypted Data Connection Internal to the VA
Veterans Information/Eligibility Record Services	Processing benefits eligibility	• Name • Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number • Personal Email Address	Encrypted Data Connection Internal to the VA

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*
		• Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Financial Information • Race/Ethnicity • Tax Identification Number • Gender • Military History/Service Connection • Alias • Benefit information • Education benefit participation, eligibility, and usage • Healthcare benefit periods of eligibility (TRICARE, CHAMPVA)	
Homeless Management Information Systems	Homeless Veteran Status Query and Response Exchange System (SQUARES 2.0)	• Name • Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number0 Personal Email Address • Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Financial Information • Race/Ethnicity • Tax Identification Number • Gender • Military History/Service Connection	Encrypted Data Connection Internal to the VA
My HealtheVet (Cloud) Assessing (Blue Button)	Correlation of Demographic data	• Name • Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number • Personal Email Address	Encrypted Data Connection Internal to the VA

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*
		• Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Financial Information • Race/Ethnicity • Tax Identification Number • Gender • Military History/Service Connection • Alias • Benefit information • Education benefit participation, eligibility, and usage • Healthcare benefit periods of eligibility (TRICARE, CHAMPVA)	
Veterans Information Solution	End-user interface system to display veteran specific benefits eligibility information	• Name • Social Security Number • Date of Birth • 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 • Race/Ethnicity • Tax Identification Number • Gender • Military History/Service Connection • Alias • Benefit information • Education benefit participation, eligibility, and usage	Encrypted Data Connection Internal to the VA

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*
		• Healthcare benefit periods of eligibility (TRICARE, CHAMPVA)	
WebGil, Veteran Outreach, Servicemembers Civil Relief Act (SCRA) Foreclosure Protection, Automated Certificate of Eligibility Loan Guaranty Service (ACELGY)	Correlation of Demographic data	• Name • Social Security Number • Date of Birth • 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 • Race/Ethnicity • Tax Identification Number • Gender • Military History/Service Connection • Alias • Benefit information • Education benefit participation, eligibility, and usage Healthcare benefit periods of eligibility (TRICARE, CHAMPVA)	Encrypted Data Connection Internal to the VA
Accessions to Military (IF#32) for Beneficiary Identification and Records Locator Subsystem (BIRLS)	This interface is to provide the mainframe-based Beneficiary Identification and Records Locator Subsystem (BIRLS) database, and the migrated BIRLS Oracle database, known as IBS, Integrated Benefit Services, hosted on VBA's (Veterans Benefits	• Name • Social Security Number • Date of Birth • 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 • Race/Ethnicity • Tax Identification Number	Encrypted Data Connection Internal to the VA

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*
	Administration) Corporate Database, with a monthly file of all persons that joined the military for the first time as active duty, guard, or reserve service members.	• Gender • Military History/Service Connection • Alias • Benefit information • Education benefit participation, eligibility, and usage • Healthcare benefit periods of eligibility (TRICARE, CHAMPVA)	
Department of Defense (DoD) Retired & Survivor Pay Reconciliation (IF#07) for Compensation Service and Pension & Fiduciary (C&P) Pay	This interface is to provide the mainframe-based Beneficiary Identification and Records Locator Subsystem (BIRLS) database, and the migrated BIRLS Oracle database, known as IBS, Integrated Benefit Services, hosted on VBA's (Veterans Benefits Administration) Corporate Database, with a monthly file of gross pay amounts for veterans in receipt of DoD retired pay and, if the veteran is deceased, their surviving spouse's survivor pay.	• Name • Social Security Number • Date of Birth • 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 • Race/Ethnicity • Tax Identification Number • Gender • Military History/Service Connection • Alias • Benefit information • Education benefit participation, eligibility, and usage • Healthcare benefit periods of eligibility (TRICARE, CHAMPVA)	Encrypted Data Connection Internal to the VA
Concierge for Care for Health Eligibility Center (HEC)	The purpose of the Concierge for Care (C4C) interface with VADIR is to provide weekly and monthly updates on separation	• Name • Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number	Encrypted Data Connection Internal to the VA

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*
	and transitioning military service members to ensure they have a complete communication of benefits available to them. Monthly extract of newly separated service members	• Personal Email Address • Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Financial Information • Race/Ethnicity • Tax Identification Number • Gender • Military History/Service Connection • Alias • Benefit information • Education benefit participation, eligibility, and usage • Healthcare benefit periods of eligibility (TRICARE, CHAMPVA)	
Performance Analysis and Integrity PA&I DoD Quarterly Separations	The legacy IF-28 and IF-42 began as 2 separate data feeds but has been combined into one data feed to cover both Return to Duty and Reserve/Guard activations and separations. This interface is from VADIR to the HINES Technology Center on a quarterly basis.	• Name • Social Security Number • Date of Birth • 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 • Race/Ethnicity • Tax Identification Number • Gender • Military History/Service Connection • Alias • Benefit information • Education benefit participation, eligibility, and usage	Encrypted Data Connection Internal to the VA

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*
		• Healthcare benefit periods of eligibility (TRICARE, CHAMPVA)	
Central Business Office (CBO) Civilian Health and Medical Program of the Department of Veteran's Affairs Reserve Retiree (CHAMPVA RES/RET) extract	Monthly data transfer between VADIR and CHAMPVA, is a bi-directional data feed with each system providing the other with data.	• Name • Social Security Number • Date of Birth • 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 • Race/Ethnicity • Tax Identification Number • Gender • Military History/Service Connection • Alias • Benefit information • Education benefit participation, eligibility, and usage • Healthcare benefit periods of eligibility (TRICARE, CHAMPVA)	Encrypted Data Connection Internal to the VA
Office of Enterprise Integration Post-9/11 population	Used for Briefing book, to build Post 911 combat veteran tab, which is viewed by various levels of personnel.	• Name • Social Security Number • Date of Birth • 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 • Race/Ethnicity • Tax Identification Number	Encrypted Data Connection Internal to the VA

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*
		• Gender • Military History/Service Connection • Alias • Benefit information • Education benefit participation, eligibility, and usage • Healthcare benefit periods of eligibility (TRICARE, CHAMPVA)	
Office of Plans and Policy Gulf War 1 Population (OPP GWI Population)	Correlation of Demographic data	• Name • Social Security Number • Date of Birth • 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 • Race/Ethnicity • Tax Identification Number • Gender • Military History/Service Connection • Alias • Benefit information • Education benefit participation, eligibility, and usage • Healthcare benefit periods of eligibility (TRICARE, CHAMPVA)	Encrypted Data Connection Internal to the VA
Office of Plans and Policy/ United States Veteran Eligibility Trends and Statistics (OPP/US VETS/Actuary Office)	Correlation of Demographic data	• Name • Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number	Encrypted Data Connection Internal to the VA

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		• Personal Email Address • Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Financial Information • Race/Ethnicity • Tax Identification Number • Gender • Military History/Service Connection • Alias • Benefit information • Education benefit participation, eligibility, and usage • Healthcare benefit periods of eligibility (TRICARE, CHAMPVA)	
Solid start, Mental Health Executive Order	Weekly (Sunday) VADIR data provided to MHEO - Mental Health Executive Order	• Name • Social Security Number • Date of Birth • 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 • Race/Ethnicity • Tax Identification Number • Gender • Military History/Service Connection • Alias • Benefit information • Education benefit participation, eligibility, and usage	Encrypted Data Connection Internal to the VA

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*
		• Healthcare benefit periods of eligibility (TRICARE, CHAMPVA)	
Suicide Prevention Center of Excellence - OAR Extract	Correlation of Demographic data	• Name • Social Security Number • Date of Birth • 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 • Race/Ethnicity • Tax Identification Number • Gender • Military History/Service Connection • Alias • Benefit information • Education benefit participation, eligibility, and usage • Healthcare benefit periods of eligibility (TRICARE, CHAMPVA)	Encrypted Data Connection Internal to the VA
Veterans Benefits Administration Performance Analysis and Integrity Office of Analytics and Reporting (VBA PA&I OAR) Extract	The OAR extract is based on combining the current VSSC data extract with additional data elements from the GW I and Post-9/11 Legacy extracts to form a single extract, produced monthly. SR-119 directs that the data extracted from VADIR to VSSC/OAR in the form of five files reflecting	• Name • Social Security Number • Date of Birth • 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 • Race/Ethnicity • Tax Identification Number	Encrypted Data Connection Internal to the VA

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*
	Person Level information (OAR_Person.txt), Military Service Level information (OAR_Mil_Svc.txt), Activation Mobilization information (OAR_GRAS.txt) Deployment Level information (OAR_Deployment.txt) Location of Deployment (OAR_Dply_Loc.txt)	• Gender • Military History/Service Connection • Alias • Benefit information • Education benefit participation, eligibility, and usage • Healthcare benefit periods of eligibility (TRICARE, CHAMPVA)	
Veterans Health Administration Office of Analytics and Reporting (VHA Policy and Planning OAR) Extract.	Correlation of Demographic data	• Name • Social Security Number • Date of Birth • 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 • Race/Ethnicity • Tax Identification Number • Gender • Military History/Service Connection • Alias • Benefit information • Education benefit participation, eligibility, and usage • Healthcare benefit periods of eligibility (TRICARE, CHAMPVA)	Encrypted Data Connection Internal to the VA

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*
VHA Portland Medical Center - OAR Extract	Correlation of Demographic data	• Name • Social Security Number • Date of Birth • 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 • Race/Ethnicity • Tax Identification Number • Gender • Military History/Service Connection • Alias • Benefit information • Education benefit participation, eligibility, and usage • Healthcare benefit periods of eligibility (TRICARE, CHAMPVA)	Encrypted Data Connection Internal to the VA
VHA Predictive Utilization for Healthcare - OAR Extract	Correlation of Demographic data	• Name • Social Security Number • Date of Birth • 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 • Race/Ethnicity • Tax Identification Number • Gender • Military History/Service Connection	Encrypted Data Connection Internal to the VA

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*
		• Alias • Benefit information • Education benefit participation, eligibility, and usage • Healthcare benefit periods of eligibility (TRICARE, CHAMPVA)	
VHA Quarterly PACT-DLI Military History Data Request	Provide quarterly VADIR data for all Veterans alive and/or deceased the last 3 years	• Name • Social Security Number • Date of Birth • 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 • Race/Ethnicity • Tax Identification Number • Gender • Military History/Service Connection • Alias • Benefit information • Education benefit participation, eligibility, and usage • Healthcare benefit periods of eligibility (TRICARE, CHAMPVA)	Encrypted Data Connection Internal to the VA
VHA Services Support Center Office of Analytics and Reporting (VSSC OAR) Extract.	Correlation of Demographic data	• Name • Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number • Personal Email Address • Emergency Contact Information (Name, Phone	Encrypted Data Connection Internal to the VA

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*
		Number, etc. of a different individual) • Financial Information • Race/Ethnicity • Tax Identification Number • Gender • Military History/Service Connection • Alias • Benefit information • Education benefit participation, eligibility, and usage • Healthcare benefit periods of eligibility (TRICARE, CHAMPVA)	
Welcome Home Packages and Education Outreach Letters for VADS	Correlation of Demographic data for welcome home packages and outreach letters	• Name • Social Security Number • Date of Birth • 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 • Race/Ethnicity • Tax Identification Number • Gender • Military History/Service Connection	Encrypted Data Connection Internal to the VA
Early Notifications (EC) and Veteran Identity & Military History for eBenefits	The purpose of the Early Communications (EC) Outreach to provide notifications to different organizations throughout the VA so that they can provide mail notifications to past	• Name • Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number Personal Email Address • Emergency Contact Information (Name, Phone	Encrypted Data Connection Internal to the VA

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*
	and present military service members.	Number, etc. of a different individual) • Financial Information • Race/Ethnicity • Tax Identification Number • Gender • Military History/Service Connection	
Veteran Identity for Loan Guaranty Service Veteran Information Portal (LGYVIP)	Produces set of separating veterans qualified for VA loans. Creates file of business events determining vets are eligible. Has table of previously sent letters.	• Name • Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number0 Personal Email Address • Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Financial Information • Race/Ethnicity • Tax Identification Number • Gender • Indemnity Compensation (DIC), award amount)	Encrypted Data Connection Internal to the VA
Veteran Identity for Stakeholder Enterprise Portal (SEP)	Correlation of demographic data.	• Name • Social Security Number • Date of Birth • 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 • Race/Ethnicity • Tax Identification Number • Gender • Military History/Service Connection	Encrypted Data Connection Internal to the VA

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*
		• Alias • Benefit information • Education benefit participation, eligibility, and usage • Healthcare benefit periods of eligibility (TRICARE, CHAMPVA)	
Veteran Relationship Management (VRM) Data Access for Veteran Identity/Eligibility Reporting System (VIERS)	Veteran Identity & Mil History	• Name • Social Security Number • Date of Birth • 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 • Race/Ethnicity • Tax Identification Number • Gender • Military History/Service Connection • Alias • Benefit information • Education benefit participation, eligibility, and usage • Healthcare benefit periods of eligibility (TRICARE, CHAMPVA)	Encrypted Data Connection Internal to the VA
Veteran Identity & Military History for Work Study Management System (WSMS)	Veteran Identity & Mil History	• Name • Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number0 Personal Email Address • Emergency Contact Information (Name, Phone	Encrypted Data Connection Internal to the VA

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*
		Number, etc. of a different individual) • Financial Information • Race/Ethnicity • Tax Identification Number • Gender • Military History/Service Connection	

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: A Privacy Risk could occur by data disclosure from end-user system.

Mitigation: Consent for use of PII data is signaled by completion and submission of any appropriate form(s) by the veteran at the point of service where VDR-AWS data is accessed by an end-user system. All VA users are trained and acknowledge usage requirements in the appropriate Rules of Behavior (RoB) documentation. Access to veteran data for use is under Title 38 U.S.C. Section 5106. All system-to-system connections are encrypted to further prevent unauthorized access to Veteran data during transmission.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
Department of Defense's Defense Manpower Data Center (DMDC) using the Defense Enrollment Eligibility Reporting System (DEERS).	Eligibility and benefits entitlement	• Name • Social Security Number • Date of Birth • 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 • Race/Ethnicity • Tax Identification Number • Gender	ISA/MOU	Encrypted data connection

		• Military History/Service Connection • Alias • Benefit information • Education benefit participation, eligibility, and usage • Healthcare benefit periods of eligibility (TRICARE, CHAMPVA)		
Prudential (VGLI, SGLI Servicing Organization)	Used to list coverage provided to Veteran and service member	• Name • Social Security Number • Date of Birth • 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 • Race/Ethnicity • Tax Identification Number • Gender • Military History/Service Connection • Alias • Benefit information • Education benefit participation, eligibility, and usage • Healthcare benefit periods of eligibility (TRICARE, CHAMPVA)	ISA/MOU	Encrypted data connection

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 of data compromise at the external location.

Mitigation: An Interconnection Security Agreement / Memorandum of Understanding (ISA/MOU) exists for both DMDC (DEERS) and Prudential Life Insurance that outlines the protective measures necessary to ensure the proper confidentiality, availability, and integrity of the stored data. These agreements are reviewed and updated as necessary, not any less often than every three years.

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.

This system provides effective notice to the public regarding its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII). It provides notice by:

1. SORN: Defense Enrollment Eligibility Reporting Systems (DEERS), DMDC 02 DoD (October 16, 2019, 84 FR 55293; corrected December 2, 2019, 84 FR 65975). DMDC-02-DoD.pdf (defense.gov) (https://www.oprm.va.gov/privacy/systems_of_records.aspx)
2. By this Privacy Impact Assessment, which is available online as required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii).

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

Defense Enrollment Eligibility Reporting Systems (DEERS), DMDC 02 DoD (October 16, 2019, 84 FR 55293; corrected December 2, 2019, 84 FR 65975). DMDC-02-DoD.pdf (defense.gov) (https://www.oprm.va.gov/privacy/systems_of_records.aspx)

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.

This Privacy Impact Assessment (PIA) serves as a public notice that VDR-AWS exists and displays/transmits individual's information. VDR-AWS uses this SORN: Defense Enrollment Eligibility Reporting Systems (DEERS), DMDC 02 DoD (October 16, 2019, 84 FR 55293; corrected December 2, 2019, 84 FR 65975). DMDC-02-DoD.pdf (defense.gov) (https://www.oprm.va.gov/privacy/systems_of_records.aspx)

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.

Individuals seeking to determine whether information about themselves is contained in this system should address written inquiries to the Deputy Director, Defense Manpower Data Center, DoD Center Monterey Bay, 400 Gigling Road, Seaside, CA 93955-6771. Signed written requests should contain the full name, identifier (i.e.,DoD ID number, DoD Benefits Number, or SSN), date of birth, and current address and telephone number of the individual. In addition, the requester must provide either a notarized statement or a declaration made in accordance with 28 U.S.C. 1746, using the following format: If executed outside the United States: "I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature)."

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.

Individuals seeking to determine whether information about themselves is contained in this system should address written inquiries to the Deputy Director, Defense Manpower Data Center, DoD Center Monterey Bay, 400 Gigling Road, Seaside, CA 93955-6771. Signed written requests should contain the full name, identifier (*i.e.* ID number, DoD Benefits Number, or SSN), date of birth, and current address and telephone number of the individual. In addition, the requester must provide either a notarized statement or a declaration made in accordance with 28 U.S.C. 1746, using the following format: If executed outside the United States: "I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature)."

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Privacy Risk: There is a risk that an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by VDR-AWS prior to providing the information to VDR-AWS.

Mitigation: The Veteran is informed during their transition from military service that the information they provided will be stored in systems that VA uses to adjudicate and grant/deny benefits, and that additional documents will be included in those collections and protected accordingly.

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.

NOTIFICATION PROCEDURES: Individuals seeking to determine whether information about themselves is contained in this system should address written inquiries to the Deputy Director, Defense Manpower Data Center, DoD Center Monterey Bay, 400 Gigling Road, Seaside, CA 93955-6771. Signed written requests should contain the full name, identifier (i.e., DoD ID number, DoD Benefits Number, or SSN), date of birth, and current address and telephone number of the individual. In addition, the requester must provide either a notarized statement or a declaration made in accordance with 28 U.S.C. 1746, using the following format: If executed outside the United States: "I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature)." If executed within the United States, its territories, possessions, or commonwealths: "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)."

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).

This is not a privacy act exempt system.

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.

VDR-AWS is a Privacy Act System.

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

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

Data is not corrected in VDR-AWS. The Veteran is required to request the data be corrected by the Department of Defense. The DoD rules for accessing records, contesting contents, and appealing initial Component determinations are contained in 32 CFR part 310, or may be obtained from the system manager. NOTIFICATION PROCEDURES: Individuals seeking to determine whether information about themselves is contained in this system should address written inquiries to the Deputy Director, Defense Manpower Data Center, DoD Center Monterey Bay, 400 Gigling Road, Seaside, CA 93955-6771. Signed written requests should contain the full name, identifier (i.e., DoD ID number, DoD Benefits Number, or SSN), date of birth, and current address and telephone number of the individual. In addition, the requester must provide either a notarized statement or a declaration made in accordance with 28 U.S.C. 1746, using the following format: If executed outside the United States: "I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature)." If executed within the United States, its territories, possessions, or commonwealths: "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)."

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.

CONTESTING RECORD PROCEDURES: The DoD rules for accessing records, contesting contents, and appealing initial agency determinations are published in 32 CFR part 310 or may be obtained from the system manager. NOTIFICATION PROCEDURES: Individuals seeking to

determine whether information about themselves is contained in this system should address written inquiries to the Deputy Director, Defense Manpower Data Center, DoD Center Monterey Bay, 400 Gigling Road, Seaside, CA 93955-6771. Signed written requests should contain the full name, identifier (i.e., DoD ID number, DoD Benefits Number, or SSN), date of birth, and current address and telephone number of the individual. In addition, the requester must provide either a notarized statement or a declaration made in accordance with 28 U.S.C. 1746, using the following format: If executed outside the United States: "I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature)." If executed within the United States, its territories, possessions, or commonwealths: "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)."

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.

CONTESTING RECORD PROCEDURES: The DoD rules for accessing records, contesting contents, and appealing initial agency determinations are published in 32 CFR part 310 or may be obtained from the system manager. NOTIFICATION PROCEDURES: Individuals seeking to determine whether information about themselves is contained in this system should address written inquiries to the Deputy Director, Defense Manpower Data Center, DoD Center Monterey Bay, 400 Gigling Road, Seaside, CA 93955-6771. Signed written requests should contain the full name, identifier (i.e., DoD ID number, DoD Benefits Number, or SSN), date of birth, and current address and telephone number of the individual. In addition, the requester must provide either a notarized statement or a declaration made in accordance with 28 U.S.C. 1746, using the following format: If executed outside the United States: "I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature)." If executed within the United States, its territories, possessions, or commonwealths: "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)."

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that a Veteran may not know how to obtain access to their records or how to request corrections to their records.

Mitigation: No changes to information within VDR-AWS are made by VA. Veterans and Veteran representatives should follow the procedures for correcting information stored in DEERS (as addressed in 7.4 above).

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 VDR-AWS; only system and database administrators have access to the server hardware and operating system.

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?

Administrators undergo a background investigation, their access is documented and verified through the MyVA Elevated Privileges Request in ePAS and associated processes, and they must agree to additional rules of behavior for system administration personnel.

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.

There is no user interface to VDR-AWS; only system and database 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 associated processes, and they must agree to additional rules of behavior for system administration personnel 64899 Information Security Role-Based Training for IT Project Managers.

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.

VDR-AWS administrators are authorized VA and contract employees. There are contractor system administration personnel within the Austin Information Technology Center (AITC) who maintain the server hardware and software but are not privileged users of the VDR-AWS system itself. Contracts are reviewed annually by the VDR-AWS Program Manager, Information System Owner, Information Owner, Contract Officer, Privacy Officer, and the Contracting Officer's Technical Representative. Contractor personnel accessing information systems must read and acknowledge their receipt and acceptance of the VA Contractor's Rules of Behavior (ROB) (for AITC technicians) prior to gaining access to any VA information system or sensitive information. The ROB includes non-disclosure and confidentiality agreements.

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.

Any 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 (for AITC technicians) 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 Talent Management System (TMS). After the user's initial acceptance of the Rules, the user must reaffirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. All VA employees must complete annual Privacy and Security training. Additional training is listed below:
TMS Course and Title
3197 Information Security Role-Based Training for IT Specialist
3867205 Training for Elevated Privileges for System Access
3867207 Information Security Role-Based Training for System Owners
1016925 Information Security Role-Based Training for Software Developers
1357076 Information Security Role-Based Training for System Administrators

4563250 PKI Certificate Management - Overview (On Demand)
1357084 Information Security Role-Based Training for Data Managers
1357083 Information Security Role-Based Training for Network Administrators
64899 Information Security Role-Based Training for IT Project Managers

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Initial Security Plan developed prior to initial ATO request.
2. *The System Security Plan Status Date:* 02-22-2023
3. *The Authorization Status:* Pending
4. *The Authorization Date:* Pending
5. *The Authorization Termination Date:* Pending
6. *The Risk Review Completion Date:* Pending
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.***

The system has not been authorized to operate as of 03-09-2023 and is currently in STEP 4 of the RMF process. The system has a FIPS 199 classification of HIGH as of 12-27-2022.

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)*

VDR-AWS utilizes the VA Enterprise Cloud (VAEC). VDR-AWS uses the Infrastructure as a Service (IaaS) model.

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.*

VAEC AWS agreement and security configuration.

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.

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.

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).

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**
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.

JULIE C. DRAKE 969177

Digitally signed by JULIE C. DRAKE 969177
Date: 2023.03.23 15:30:43 -06'00'

Privacy Officer, Julie Drake

Eric Abraham 3564094

Digitally signed by Eric Abraham 3564094
Date: 2023.03.23 14:53:10 -05'00'

Information System Security Officer, Abraham Eric

Alexander V. Torres 693173

Digitally signed by Alexander V. Torres 693173
Date: 2023.03.22 09:04:11 -07'00'

Information System Owner, Torres Alexander

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.

Defense Enrollment Eligibility Reporting Systems (DEERS), DMDC 02 DoD (October 16, 2019, 84 FR 55293; corrected December 2, 2019, 84 FR 65975). DMDC-02-DoD.pdf (defense.gov) (VA Privacy Service) VBA Corporate:

58VA21/22/28 86 FR 61858 (11/8/2021) Compensation, Pension, Education and Vocational Rehabilitation and Employment Records-VA (2021-24372.pdf (govinfo.gov))

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