Privacy Impact Assessment for the VA IT System called:

VA DoD Identity Repository (VADIR/VDR)

Veterans Relationship Management (VRM)
Veterans Benefits Administration (VBA)

Date PIA submitted for review:

04/20/2022

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 (VDR) 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 all the data within VDR. The VDR 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 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 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:

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

The Veterans Affairs (VA) Department of Defense (DoD) Identity Repository (VDR) system is owned by the Veterans Relationship Management (VRM) program and maintained by IT Operations (ITOPS), Service Operations, Infrastructure Operations (IO), Platform Support.

VDR 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. The VDR 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 stores information on approximately 13 million Veterans.

DoD owns the data and has exclusive disposition and retention of all data records. VDR 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 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 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 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 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 (138VA005Q). VDR does not use cloud technology.

Section 1. Characterization of the Information

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

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

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

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.
This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

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

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

☒ Name
☒ Social Security Number
☒ Date of Birth
☐ Mother's Maiden Name
☒ Personal Mailing Address
☒ Personal Phone Number(s)
☒ Personal Fax Number
☒ Personal Email Address
☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☐ Financial Account Information
☐ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☐ Current Medications
☐ Previous Medical Records
☒ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☒ Gender
☐ Integration Control Number (ICN)
☒Military History/Service Connection
☐ Next of Kin
☒ Other Unique Identifying Information (list below)

Member's maiden name, alias, family relations, service information, education, and benefit information are also collected. Veteran's record may include identifying information (e.g., name, contact information, SSN), association to dependents, cross reference to other names used, military service participation and status information (branch of service, rank, enter on duty date, release from active duty date, military occupations, type of duty, character of service, awards), reason and nature of active duty separation (completion of commitment, disability, hardship, etc.) combat/environmental exposures (combat pay, combat awards, theater location), combat deployments (period of deployment, location/country), Guard/Reserve activations (period of activation, type of activation), military casualty/disabilities (line of duty death, physical examination board status, serious/very serious injury status, DoD rated disabilities), education benefit participation, eligibility and usage, healthcare benefit periods of eligibility (TRICARE, CHAMPVA), and VA compensation (rating, Dependency and Indemnity Compensation (DIC), award amount).

PII Mapping of Components

VA DoD Identity Repository consists of one key component (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 and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

Note: Due to the PIA being a public facing document, please do not include the server names in the table.

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
VDRP	Yes	Yes	Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Number, Fax Number, email Address, Race/ethnicity, Member's maiden name, alias, family relations, service information, education, benefit information, association to dependents, cross reference to other names used, military service participation and status, information (branch of service, rank, enter on duty date, release from active-duty date, military occupations, type of duty, character of service, awards), reason	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	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.)

			and nature of active duty separation (completion of commitment, disability, hardship, etc.) combat/environmental exposures (combat pay, combat awards, theater location), combat deployments (period of deployment, location/country), Guard/Reserve activations (period of activation, type of activation), military casualty/disabilities (line of duty death, physical examination board status, serious/very serious injury status, DoD rated disabilities), education benefit participation, eligibility and usage, healthcare benefit periods of eligibility (TRICARE, CHAMPVA), and VA compensation (rating, Dependency and Indemnity Compensation (DIC), award amount).	Uniformed Services (CHAMPUS) benefits.	We have multiple transfer methods. I'll see if there is a better name for the data at rest than Oracle Security.

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

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

Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.

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

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

1.3 How is the information collected?

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

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

VDR 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.

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

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

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

VDR assumes that information was checked for accuracy when it was first entered into the host system. 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 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: Because VDR 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: VADIR 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 VADIR 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?

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

If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the

individual? If so, explain fully under which circumstances and by whom that information will be used.
This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

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

2.3 How is the information in the system secured?

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

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

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

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

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. All these systems are regularly scanned to ensure proper security procedures are in place.

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

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

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

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

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

Add answer here:

No user access within VDR exists. 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

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 retained on the VDR system: Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Numbers, Fax numbers, Email Addresses, Member's maiden name, alias, family relations, service information, education, Veteran's record may include identifying information (e.g., name, contact information, SSN), association to dependents, cross reference to other names used, military service participation and status information (branch of service, rank, enter on duty date, release from active duty date, military occupations, type of duty, character of service, awards), reason and nature of active duty separation (completion of commitment, disability, hardship, etc.) combat/environmental exposures (combat pay, combat awards, theater location), combat deployments (period of deployment, location/country), Guard/Reserve activations (period of activation, type of activation), military casualty/disabilities (line of duty death, physical examination board status, serious/very serious injury status, DoD rated disabilities), education benefit participation, eligibility and usage, healthcare benefit periods of eligibility (TRICARE, CHAMPVA), and VA compensation (rating, Dependency and Indemnity Compensation (DIC), award amount). The record of an individual included in this system may be provided to DoD systems or offices for use in connection with matters relating to one of DoD's programs to enable delivery of healthcare or other DoD benefit to eligible beneficiaries. The name, address, VA file number, date of birth, date of death, social security number, and service information may be disclosed to DoD's DMDC. DoD will use this information 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. All information collected is retained.

3.2 How long is information retained?

In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

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

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.

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

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

DoD owns the data and has exclusive disposition and retention of all data records. VDR 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.

The records control for the VDR system hardware and user logs is GRS 4.2: Information Access and Protection Records Item 130 located at https://www.archives.gov/records-mgmt/grs.html.

GRS 4.2: Information Access and Protection Records: This schedule covers records created in the course of agencies (1) responding to requests for access to Government information and (2) protecting information that is classified or controlled unclassified or contains personal data that is required by law to be protected.
Item 130 - Personally identifiable information extracts. System-generated or hardcopy printouts generated for business purposes that contain Personally Identifiable Information. Disposition Instruction: Temporary. Destroy when 90 days old or no longer needed pursuant to supervisory authorization, whichever is appropriate.

3.4 What are the procedures for the elimination of SPI?

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

Data is not removed from VDR. The DoD owns the data record and is responsible for all disposition of the data.

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

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

VDR does not use PII for training or testing but does for research.

VDR isn't an application; rather, it's a database, and as such, no training ever takes place. It's simply a tool that hosts data. Testing on VDR does occur, but solely in the Dev and Test environments, where fictional test data is used. No real world PII will ever be found in the Dev and Test environments. PII is used for research, however, as statisticians, doctors, and epidemiologists need access to PII to work with the service members or veterans they're studying. All Service Requests are reviewed to insure if PII information is requested, the PII is required for said customer to execute their task. If PII is required, customers/requestors are asked to document why the PII is required and how it is being used. If and when there is a conflict or question about the use of PII, it is escalated to the ISSO for review and approval. Due to this, all personnel with access to Veteran's information, including the PII found in VDR, are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually. This ensures that researchers with access to Veteran's data, and PII specifically, know the rules of engagement with this data, and the consequences for violating those rules. Also, before even getting access to this data, researchers must be cleared by the Privacy Office at the VA Medical Center (VAMC).

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

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.

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

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

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

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

Follow the format below:

<u>Privacy Risk:</u> There is a risk that a veteran would be concerned the VA was changing or deleting their data

<u>Mitigation:</u> The DoD owns the data and is responsible for disposition and retention of the data records. VADIR 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, which includes how long to retain the data. VA only reads the data. In general, the VADIR data is an historical record of an individual's service to their country and as such is kept into perpetuity.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Veterans Information Solution (VIS)	End-user interface system	Veteran demographic information	Secure web (HTTPS)
Veteran Information/Eligibility Records Services (VRS)	Processing benefits eligibility	Benefit-related information	Encrypted data connection
Beneficiary Identification and Records Locator (BIRLS)	Permanent storage location of additional data	Veteran DD-214, Accessions to Military	Encrypted data connection
Stakeholder Enterprise Portal	Correlation of demographic data	Veteran demographic information	Encrypted data connection
VA Office of Enterprise Integration (OEI) (formerly Office of Policy and Planning)	Correlation of demographic data	Veteran demographic information	Aviation and Missile Research, Development, and Engineering Center Safe Access File Exchange (AMRDEC SAFE)
VBA Insurance Service	Correlation of demographic data	Veteran demographic information	Encrypted data connection
VBA Loan Guaranty Service	Correlation of demographic data	Veteran demographic information	Encrypted data connection

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***
VBA Office of Performance Analysis and Integrity	Correlation of demographic data	Veteran demographic information	Encrypted data connection
Veterans Health Administration (VHA) Health Eligibility Center (HEC) Enrollment System	Correlation of demographic data	Veteran demographic information	Encrypted data connection
VBA Reserve Educational Assistance Program	Correlation of demographic data	Veteran demographic information	Encrypted data connection
VBA Compensation Service & Pension and Fiduciary Service	Correlation of demographic data	Veteran demographic information	Encrypted data connection
VBA Education Services	Correlation of demographic data	Veteran demographic information	Encrypted data connection
VHA Health Administration Center	Correlation of demographic data	Veteran demographic information	Encrypted data connection
VHA Support Services Center Office of Analytics and Reporting	Correlation of demographic data	Veteran demographic information	Encrypted data connection
VHA Environmental & Epidemiology Service	Correlation of demographic data	Veteran demographic information	Encrypted data connection
VA Allocation Resource Center	Correlation of demographic data	Veteran demographic information	Encrypted data connection
VA Information Resource Center	Correlation of demographic data	Veteran demographic information	Encrypted data connection
VA Profile	Correlation of demographic data	Veteran demographic information	Encrypted data 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.
This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: 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 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	*List the purpose of*	*List the specific PII/PHI data elements that are processed*	*List the legal*	*List the method of*

or IT System information is shared/received with	***information being shared / received / transmitted with the specified program office or IT system***	***(shared/received/transmitted)with the Program or IT system***	***authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***transmission and the measures in place to secure data***
Defense Manpower Data Center (DMDC) / Defense Enrollment Eligibility Reporting System (DEERS)	Eligibility and benefits entitlement	The data transmitted may include Identifying information (e.g., name, contact information, current and any prior Social Security number), association to dependents, cross reference to other names used, military service participation and status information (branch of service, rank, enter on duty date, release from active-duty date, military occupations, type of duty, character of service), reason and nature of active-duty separation (Completion of commitment, disability, hardship, etc.), combat-related (Combat pay, theater location), combat deployments (period of deployment, location/country), Guard/Reserve activations (period of activation, type of activation), military casualty/disabilities (Line of duty death, DoD rated disability percent), education benefit participation, eligibility, and usage, pay data, including military pay, separation pay, retired pay, Reserve drill pay, and survivors pay, Servicemembers Group Life Insurance coverage, VA compensation (rating, Dependency, and Indemnity Compensation (DIC), award amount), and veteran mailing address.	ISA/ MOU	Encrypted data connection
The Prudential Life	Used to list	Servicemember and spouse SGLI Coverage information, military	ISA/ MOU	Secure data transfer

Insurance	coverage provided to Veteran and service member	Disability information, including sensitive personal information (SPI).		

5.2 <u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>

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:

<u>Privacy Risk:</u> There is a risk of data compromise at the external location.

<u>Mitigation:</u> 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 notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

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

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

Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection. This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

VDR SORN 138VA005Q is published in the Federal Register, which is available to the public. Veterans Affairs/Department of Defense Identity Repository (VADIR)-VA. E9-17776.pdf (govinfo.gov). OPRM link: Current SORN List (va.gov)

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

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

Any opportunity to decline providing information occurs at different points in the intake process as the Veteran transitions from military service. These points occur before the data is transferred into the VDR database.

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

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

Veterans do not have the right to consent to any data stored into VDR specifically. Instead, their consent is exercised when they transition from the military.

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.

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

<u>Principle of Transparency:</u> Has sufficient notice been provided to the individual?

<u>Principle of Use Limitation:</u> 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 a Veteran may not know that their information may be entered into a long-term records storage system.

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?

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

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

If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.
This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

Veteran access is dependent on pre-screening through Defense Enrollment Eligibility Reporting System (DEERS) and acquiring a Department of Defense Self-Service Logon (DS Logon) account.

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. The Veteran is required to request the data be corrected by the Department of Defense.

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.

Under the jurisdiction of VHA, VHA Handbook 1605.1 Appendix D 'Privacy and Release Information', section 8 states the rights of the Veterans to amend to their records via submitting VA Form 10-5345a, Individual's Request For a Copy of Their Own Health Information, may be used as the written request requirement, which includes designated record sets, as provided in 38 CFR 1.579 and 45 CFR 164.526. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and be filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

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

To change data stored in VDR, the Veteran would have to contact their local Military Personnel Facility, DEERS office at a Military Treatment Facility, or exercise their DS Logon to make the change through DEERS.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that a 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 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?

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

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

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

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

There is no user interface to VDR; 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.

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 administrators may be authorized VA and contract employees. There are contract system administration personnel within the Austin Information Technology Center (AITC) who maintain the server hardware and software. Contracts are reviewed annually by the VDR Program Manager, Information System Owner, Information Owner, Contract Officer, Privacy Officer, and the Contracting Officer's Technical Representative.

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.

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

If Yes, provide:

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

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

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

The system has an approved SSP dated 12-28-2021.
The most current approved Authorization Date is 02-26-2022 with a termination date of 08-25-2022.
The Risk Review was completed on 02-18-2022.
VDR has a FIPS 199 classification of HIGH.

Section 9 – Technology Usage

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

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

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS).

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

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1.

VDR does not use Cloud Technology currently. A request has been submitted for VDR migration to the cloud environment.

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

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

VDR does not use Cloud Technology currently.

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.

VDR does not use Cloud Technology currently.

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.

VDR does not use Cloud Technology currently.

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).

VDR does not use Robotics Process Automation (RPA).

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

JULIE C. DRAKE 969177

Digitally signed by JULIE C. DRAKE 969177
Date: 2022.05.25 10:44:03 -06'00'

Privacy Officer, Julie Drake

Eric Abraham 3564094

Digitally signed by Eric Abraham 3564094
Date: 2022.05.25 12:00:54 -05'00'

Information System Security Officer, Abraham Eric

Alexander V. Torres 693173

Digitally signed by Alexander V. Torres 693173
Date: 2022.05.31 12:11:20 -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).

https://www.gpo.gov/fdsys/pkg/FR-2009-07-27/pdf/E9-17776.pdf

VDR SORN 138VA005Q is published in the Federal Register, which is available to the public. Veterans Affairs/Department of Defense Identity Repository (VADIR)-VA. E9-17776.pdf (govinfo.gov). OPRM link: Current SORN List (va.gov)