Privacy Impact Assessment for the VA IT System called:

Readiness and Employment System

Veterans Benefits Administration (VBA)

Veteran Readiness and Employment (VR&E)

Date PIA submitted for review:

09/22/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Renu Roy	renu.roy@va.gov	202-263-9119
Information System Security Officer (ISSO)	Andrew Vilailack	andrew.vilailack@va.gov	813-970-7568
Information System Owner	Robert M. Cervantes	robert.cervantes@va.gov	202-769-6131

Abstract

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

Readiness and Employment System (RES) is seeking to replace its legacy case management system with a modern case management platform that leverages automation. RES will allow Veteran Readiness and Employment (VR&E) staff to support program participants to successfully prepare for, find, and maintain gainful employment by significantly improving the way counselors deliver services to Veterans. This solution should be fully integrated with existing VA/VBA systems, providing a near single point of entry for counselors. RES is focused on data to ensure VR&E leadership has the business insight at all times to make informed business decisions faster.

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.
Readiness and Employment System. Veteran Readiness and Employment (VR&E) Service

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

Enables Vocational Rehabilitation Counselor (VRC) engagement, data entry and documentation within a VA Enterprise Cloud (VAEC), Amazon Web Services (AWS), Government Cloud. The solution will be used to manage the workload of field staff in the delivery of services and benefits to entitled Veterans with service-connected disabilities to obtain and maintain suitable employment and, if not employable, achieve independence in daily living to the maximum extent feasible.

C. Indicate the ownership or control of the IT system or project.
VA Owned and VA Operated

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.
Current program participant level is approximately 130,000. VR&E Service anticipates increases to this level by the PACT Act, as well as the results of outreach events. Participation in VR&E is voluntary.

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

Veterans' name, address, phone number, social security number, authoritative military service data, etc. The purpose of collecting this data is to help manage the workload of Vocational Rehabilitation Counselors (VRC) to provide all services and assistance necessary to enable eligible Veterans with service-connected disabilities to obtain and maintain suitable employment and, if not employable, achieve independence in daily living to the maximum extent feasible.

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

Systems that Readiness and Employment System (RES) will integrate with include: VAF 28-1900 claim application – To process Name, SSN, VA File Number, DOB, Mailing Address, Zip Code, Email address, Phone number, and Number of years of education; VA Profile - To process Name, SSN, DOB, Personal Mailing Address, Zip Code, Personal Email address, Personal Phone number, Gender, Race, Race, Religion, Marital Status, Ethnicity, Preferred language, Administrative Service Episodes, Disability information/ratings, Military ratings; Corporate Database (CorpDB) – To process Dependent information, Entitlement Data Veteran Sensitivity Level, and Power of Attorney (POA); MPI (Master Person Index) – To process Name, SSN, DOB, Personal Mailing Address, Zip Code, Phone number, Self-Identified Gender, Birth sex, Place of Birth; Hard-copy paper forms – To process Name, SSN, DOB, Mailing Address, Zip Code, Email address, Phone number; Benefits Delivery Network (BDN) – To process Only reading 'Entitlement Data' remaining/used from BDN tables residing in Corp DB; VA.gov - To process Name, SSN, DOB, Mailing Address, Zip Code, Email address, Phone number, VA File Number, Number of years of education; Long Term Solution (System)(LTS) – To process Veterans entitlements; Electronic Virtual Assistant Scheduler(e-VA Scheduler) – To process Veteran first name, Veteran last name, Veteran phone number, Veteran communication preferences, Veteran VA forms , Veteran VA letters ; Electronic Folder(e-Folder) – To process Veteran forms and letters; Identity and Access Management System (IAM) – To process Username from VA Active directory; Centralized Administrative Accounting Transaction System (CAATS) – To process Card Number – last 6 digits, Card holder name, Veteran first name, Veteran last name, Purchase Card Reconciliation data, Payment Mechanism; Centralized Mail Portal (CMP) – To process Name, SSN, DOB, Mailing Address, Zip Code, Email address, Phone number, VA File Number, Number of years of education; HINES – To process Veteran forms and letters data, Name, SSN, DOB, Mailing Address, Zip Code, Email address, Phone number, VA File Number; Enterprise Management of Payments, Workload, and Reporting (eMPWR) – To process FNOD (First Notice of Death), Incarceration, Veteran award data, Veteran payment data.

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

The Vocational Rehabilitation Counselors (VRCs) will be using the Readiness and Employment System (RES) and will be in different Regional Offices (ROs) nationwide.

3. Legal Authority and SORN

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

https://department.va.gov/privacy/
58VA21/22/28 86 FR 61858: SORN Name: Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA
https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

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?

Readiness and Employment System SORN does not require amendment or revision and approval. RES uses Cloud Technology. RES is hosted in the VA Enterprise Cloud VA Enterprise Cloud (VAEC), Amazon Web Services (AWS), Government Cloud.

D. System Changes

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

No. The PIA will not result in a circumstance that will require a change in the System.

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

No. The PIA will not result in a circumstance that will require a change in the System.

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)

Service number, rank, total amount of active service, whether Veteran was discharged with a disability, received a Purple Heart or other military decoration, Number of years of education, Religion, Marital Status, Preferred language, Dependent information, Entitlement Data, Veteran Sensitivity Level, Self-Identified Gender, Birth sex, Place of Birth, Only reading 'Entitlement Data' remaining/used from BDN tables residing in Corp DB, Original Entitlement, Used Entitlement, Transferred entitlement to the dependents, Entitlement used by the dependents, Administrative Service, Episodes, Disability, information/ratings, Military ratings, Veteran communication preferences, Veteran VA forms, Veteran VA letters, Username from VA Active directory, Card Number – last 6 digits, Card holder name, Purchase Card Reconciliation data, FNOD (First Notice of Death), Incarceration, VA Employee name assisting the Veterans, VA File Number, Power of Attorney (POA), Veteran Service Organization (VSO). Award history; Codes and description for the awards; Veteran award data; Veteran payment data; Payment Mechanism.

*Specify type of Certificate or License Number (e.g. Occupational, Education, Medical) Occupational, Education.

PII Mapping of Components (Servers/Database)

Readiness and Employment System consists of about 16 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 Readiness and Employment System 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
VAF 28-1900 claim application Data source: VBMS Context: Claim applications that are sent via va.gov (veterans sending electronic applications) and CMP (veterans sending manual applications) are now both retrieved from VBMS integration	Yes	Yes	Name, SSN, VA File Number, DOB, Mailing Address, Zip Code, Email address, Phone number, Number of years of education	Determine eligibility for Veteran compensation	Limited number of Counselors / Admin Users. All Counselors / Administrative Users undergo mandated annual security and privacy training
VA Profile	Yes	Yes	Name, SSN, DOB, Personal Mailing Address, Zip Code, Personal Email address, Personal Phone number, Gender, Race, Religion, Marital Status, Ethnicity, Preferred language, Administrative Service Episodes, Disability information/ratings, Military ratings	To process health related information of Users	All Counselors / Administrative Users undergo mandated annual security and privacy training
Corporate Database (CorpDB)	Yes	Yes	Dependent information, Entitlement Data	To process health related information of Users	All Counselors / Administrative Users undergo mandated annual

			Veteran Sensitivity Level, Power of Attorney (POA)		security and privacy training
MPI (Master Person Index)	Yes	Yes	Name, SSN, DOB, Personal Mailing Address, Zip Code, Phone number, Self-Identified Gender, Birth sex, Place of Birth	To process health related information of Users	All Counselors / Administrative Users undergo mandated annual security and privacy training
Hard-copy paper forms	Yes	Yes	Name, SSN, DOB, Mailing Address, Zip Code, Email address, Phone number	To process health related information of Users	All Counselors / Administrative Users undergo mandated annual security and privacy training

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

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

The Personal Identifiable Information (PII) and Sensitive Personal Information (SPI) listed above is synced directly from the Veterans Benefits Management System (VBMS) database. When the Vocational Rehabilitation Counselors (VRCs) request changes to this information, they must contact the Service Center directly.

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.

RES uses Veterans Benefits Management System (VBMS) to look up address, duty status changes, awards information, and other information in order to update the Veterans' case information.

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

The data collected by RES are from different sources. The first by the first of automated input VAF 28-1900 claim application. VA counselors at the remote offices (RO) request information from veterans to enter on the forms. The second source of data collected by RES is from hard-copy paper forms. A veteran can enter the required information on paper forms and submit the

forms personally via Postal Mail or submitted via Fax Machine. Next is the VA Profile. Veterans create and input the required information. Another source is the Corporate Database (CorpDB). Veterans can enter the required information. Another source is the MPI (Master Person Index). Veterans can enter the required information.

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? Yes. The original data is entered by veterans into apps or by VA counselors who enter the data for veterans. There are many VA forms used by Veterans to apply for and/or make adjustments to pending benefits, which are the only means of collecting the Veteran information. The information on these forms is entered by the veteran or counselor onto automated screens provided by applications and is stored into the corporate database. The information is collected primarily on defined forms and entered to specific fields of the corporate database records in support of solutions that provide electronic "eFolders" for claims processing through imaging, document management technologies and integration with output capabilities of several other VA systems.VA Form 28-1900, Application for Vocational Rehabilitation Benefits; Form 21-4142, Authorization and Consent to Release Information to the Department of Veterans Affairs (VA) are specifically used by veterans to request rehabilitation or education benefits. All VBA benefit forms are located at http://www.va.gov/vaforms/. The URL of the associated privacy statement is: http://www.va.gov/privacy/. VBA forms can be downloaded from this site, filled in and printed to be delivered in paper form. All collected information is used to determine eligibility for benefits, process ratings and to provide payments via the Department of Treasury. The VBA toll free number for veterans is 1-800-827-1000. Clients are referred to and transferred to the Regional Office of Jurisdiction, where they can provide a service representative with required information. All collected information is used to determine eligibility for benefits, process ratings and to provide payments via the Department of Treasury. VBA employees may also contact a Veteran directly to obtain clarifying information for a claim for benefits.

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.

Veterans Benefits Management System (VBMS) is the authoritative source of Veterans' Personal Identifiable Information (PII) for the Veterans Affairs (VA)

The information is also obtained from https://www.ebenefits.va.gov.

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.

Original submission of data is verified for completeness by the Regional Office Case Managers. There are also internal program controls, edits, and checks to ensure that the data submitted is complete. Forms are also visually examined.

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.

Automated edits and audits determine that a) a data element is present, and b) that the value is consistent with the data requested, and c) consistent with the record being created/updated.

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect

Title 10 U.S.C. chapters 106a, 510,1606 and 1607 and Title 38, U.S.C. Section 501(a) and Chapters 11, 13, 15,18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51,53, and 55 provide the legal authority for operating the WINRS components. VA gathers or creates these records in order to enable it to administer statutory benefits programs to Veterans, Service members, reservists, and their spouses, surviving spouses, and dependents, who file claims for a wide variety of Federal Veteran's benefits administered by VA.

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:

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

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: Sensitive Personal Information including personal contact information, service information and benefit information may be released to unauthorized individuals.

Mitigation: The RES application adheres to the information security requirements instituted by the VA Office of Information Technology (OIT).
•All employees with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.

Section 2. Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe how the information in the system will be used in support of the program's business purpose.

Identify and list each use (both internal and external to VA) of the information collected or maintained. This question is related to privacy control AP-2, Purpose Specification.

The information collected from the Veteran is used to determine the level of benefit received by the Veteran. Benefits include compensation, rehabilitation support, and education. Additionally, diagnostic codes and percent of disability determine eligibility for specially adapted housing; determine appropriate modifications under specially adapted housing program. The collected information is used to identify and track a Veteran (or a family member such as a surviving spouse), correspond with a Veteran, coordinate compensation, education, rehab medical support, or generate historical reports.

The following information is collected:

Service number, rank, total amount of active service, whether Veteran was discharged with a disability, received a Purple Heart or other military decoration, Number of years of education,

Religion, Marital Status, Preferred language, Dependent information, Entitlement Data, Veteran Sensitivity Level, Self-Identified Gender, Birth sex, Place of Birth, Only reading 'Entitlement Data' remaining/used from BDN tables residing in Corp DB, Original Entitlement, Used Entitlement, Transferred entitlement to the dependents, Entitlement used by the dependents, Administrative Service, Episodes, Disability, information/ratings, Military ratings, Veteran communication preferences, Veteran VA forms, Veteran VA letters, Username from VA Active directory, Card Number – last 6 digits, Card holder name, Purchase Card Reconciliation data, FNOD (First Notice of Death), Incarceration, VA Employee name assisting the Veterans, VA File Number, Power of Attorney (POA), Veteran Service Organization (VSO). Award history; Codes and description for the awards; Veteran award data; Veteran payment data; Payment Mechanism

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.

Data are checked for completeness by system audits, manual verifications, and annual questionnaires through automated Veteran letters. These letters ask specific questions for verification based on the existing entitlement or benefit the Veteran is receiving. Also, data are updated with each Veteran correspondence.

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.

Data are updated because of returned mail, or returned direct deposits, or through contact with the Veteran, beneficiary, or power of attorney. All data are matched against supporting claims documentation submitted by the Veteran, widow, or dependent. Certain data such as SSN is verified with the Social Security Administration. Prior to any award or entitlement authorization(s) by the VBA, the Veteran record is manually reviewed, and data validated to ensure correct entitlement has been approved.

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?

RES uses corporate database and uses the VBA specified Tuxedo services to communicate with the corporate database. Users are required to go through the Common Security Login mechanism to access the application and the data.

In Transit: TLS 1.2 is a Transport Layer Security 1.2 protocol in networking that uses AES 256 (Advanced Encryption Standard) data encryption methods to encrypt the data while transferring it to the recipient. AES 256 is one of the most secure methods for encrypting sensitive data sent over the internet.

At Rest: Amazon RDS encrypted DB instances use the industry standard AES-256 encryption algorithm to encrypt your data on the server that hosts your Amazon RDS DB instances. Amazon RDS handles authentication of access and decryption of your data transparently with a minimal impact on performance.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?
Yes. Social Security Numbers (SSNs) are encrypted while in transit and at rest.

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

RES uses corporate database and uses the VBA specified Tuxedo services to communicate with the corporate database. Users are required to go through the Common Security Login mechanism to access the application and the data. This is another VBA provided security measure. SSN are encrypted while in transit only.

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?
The SORN defines the information collected from veterans, use of the information, and how the information is accessed and stored. The information collected is used for determining a veteran's benefits, such as compensation or education. The security controls for the RES application cover 17 security areas regarding protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification an d authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity.

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

2.4c *Does access require manager approval?* Yes

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

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

The RES application team has implemented the required security controls based on the tailoring guidance of NIST Special Publication 80053 and VA directives or handbooks. VA Records Management Policy and the VA Rules of Behavior in Talent Management System (TMS) govern how veterans' information is used, stored, and protected.

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

*Identify and list all information collected from question 1.1 that is **retained** by the system.*
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal
Name, Social Security Number, Date of Birth, Mother's Maiden Name, Mailing Address, Zip Code, Phone Numbers, Email Addresses, Financial Account Information, Current Medications, Previous Medical Records. RES does not store data but uses data from established systems in VA such as CorpDB.

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.*

Compensation, pension, and vocational rehabilitation claims folders are retained at the servicing regional office until they are inactive for three years, after which they are transferred to the Records Management Center (RMC) for the life of the Veteran. Official legal documents (e.g., birth certificates, marriage licenses) are returned to the claimant after copies are made for the claimant's file. At the death of the veteran, these records are sent to the Federal Records Center (FRC) and maintained by the National Archives and Records Administration (NARA) in accordance with NARA policy. Some claims folders are electronically imaged; in which case, the electronic folder is maintained in the same manner as the claims folder. Once a file is electronically imaged and accepted by VBA, its paper contents (with the exception of documents that are the official property of the Department of Defense, and official legal documents), are destroyed in accordance with Records Control Schedule VB–1 Part 1 Section XIII, as authorized by NARA. Documents that are the property of the Department of Defense are either stored at the RMC or transferred to NARA and maintained in accordance with NARA policy. Vocational Rehabilitation counseling records are maintained until the exhaustion of a Veteran's maximum entitlement or upon the exceeding of a Veteran's delimiting date of eligibility (generally, ten or twelve years from discharge or release from active duty), whichever occurs first, and then destroyed. Automated storage media containing temporary working information are retained until a claim is decided, and then destroyed. All other automated storage media are retained and disposed of in accordance with disposition authorization approved by NARA. Education electronic folders are retained at the servicing Regional Processing Office. Education folders may be destroyed in accordance with the times set forth in the Veterans Benefits Administration Records Management, Records Control Schedule VB–1, Part 1, Section VII, as authorized by NARA. Employee productivity records are maintained for two years after which they are destroyed by shredding or burning.

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

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

The VA procedures for eliminating data are available from the VBA Records Control Schedule, VB1. The retention schedule has been approved by the National Archives and Records Administration (NARA). VBA Records Management, Records Control Schedule VB-1, Part 1, Section VII as authorized by NARA

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.

Records/digital information will be eliminated following the sanitization procedures in VA 6300 Records and Information Management and VA 6500.1 Electronic Media Sanitization. Paper records are destroyed on-site weekly. Paper records are shredded using an approved National Security Agency (NSA) High Security Crosscut Shredder from the NSA High Security Crosscut Shredder List.

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.

VA Handbook 6500 mandates that Systems under development should not process "live data" or do any real processing in which true business decisions will be based. Test data that is de-identified should be used to test systems and develop systems that have not yet undergone security Authorization and Authentication (A&A). Furthermore, systems that are in development (pilot, proof-of-concept, or prototype) should not be attached to VA networks without first being assessed and authorized. Additionally, VA wide Directive 6511 describes the responsibilities, requirements, and procedures for eliminating PII or information exempt from release under FOIA from presentations that may be seen by non-VA parties. This Directive includes guidance for conducting privacy reviews of presentations, and the criteria for when presenters must self-certify that their presentations are devoid of PII, or information exempt from release under FOIA.

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. (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: As described herein, support systems retain information until that work in progress is completed and data is committed to master systems and records. The master systems retain data on a permanent basis (beyond the actual death of the veteran). If a master system is to be deactivated, critical information is migrated to the new system and the old system along with associated data is archived according to the application disposition worksheet. As such, SPI, PII or PHI may be held for long after the original record was required to be disposed. This extension of retention periods increases the risk that SPI may be breached or otherwise put at risk. RES does not store data, but uses data from other established systems in VA, such as CorpDB.

Mitigation: Redaction of some information is required by law and protects the privacy interest of any individual who may have SPI, PII or PHI which may appear in the data and files collected. All personnel with access to the veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior Training annually.

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 transmitta l***
Corporate Database (CorpDB)	-To retrieve Veterans data -Insert updated Veterans data for all VA RES integrated data systems / applications	Dependent information Entitlement Data Sensitivity Level Power of Attorney (POA)	Electronic transmission
Benefits Delivery Network (BDN)	To retrieve Veterans data -Insert updated Veterans data for all VA RES integrated data systems / applications	Only reading 'Entitlement Data' remaining/used from BDN tables residing in Corp DB	Electronic transmission
VA.gov	To intake electronic Ch 31 claim application	Name, SSN, DOB, Mailing Address, Zip Code, Email address, Phone number, VA File Number, Number of years of education	Electronic transmission

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 transmitta l***
Long Term Solution (System) (LTS)	To calculate remaining Entitlement for the Veterans.	Veteran: Original Entitlement, Used Entitlement Recurring Payments made to Program Participant: a. Award history i. Approved awards created in LTS for the Veteran b. Codes and description for the awards Benefit Level Used Entitlement: a. If the entitlement is transferred- RES need that data, not limiting to below: b. Transferred entitlement to the dependents c. Entitlement used by the dependents	Electronic transmission
VA Profile	To determine Veteran Eligibility to receive Ch 31 benefits	Name, SSN, DOB, Personal Mailing Address, Zip Code, Personal Email address, Personal Phone number, Gender, Race, Religion, Marital Status, Ethnicity, Preferred language, Administrative Service, Episodes, Disability, information/ratings, Military ratings	Electronic transmission
Electronic Virtual Assistant Scheduler (e-VA Scheduler)	To comunícate with the Veteran electronically.	Veteran first name Veteran last name Veteran phone number Veteran communication preferences Veteran VA forms Veteran VA letters	Electronic transmission

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 transmitta l*
Electronic Folder (e-Folder)	For Veteran document repository	Veteran forms and letters	Electronic transmission
Identity and Access Management System (IAM)	For RES user authentication	Username from VA Active directory	Electronic transmission
Centralized Administrative Accounting Transaction System (CAATS)	Intake Purchase order authorizations	Card Number – last 6 digits, Card holder name, Veteran first name, Veteran last name, Purchase Card Reconciliation data, Payment Mechanism	Electronic transmission
Centralized Mail Portal (CMP)	To intake paper form of Ch 31 claim applications	Name, SSN, DOB, Mailing Address, Zip Code, Email address, Phone number, VA File Number, Number of years of education	Electronic transmission
HINES	To mail our award letters to the Veterans (POAs/dependents)	Veteran forms and letters data, Name, SSN, DOB, Mailing Address, Zip Code, Email address, Phone number, VA File Number	Electronic transmission
Enterprise Management of Payments, Workload, and Reporting (eMPWR)	To make award payments to the Veterans	FNOD (First Notice of Death), Incarceration, Veteran award data, Veteran payment data	Electronic transmission
Master Person Index (MPI)	Validate Veteran's record in VA systems	Name, SSN, DOB, Personal Mailing Address, Zip Code, Phone number, Self-Identified Gender, Birth sex, Place of Birth	Electronic transmission

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: There is a risk that RES data may be shared with unauthorized users or authorized users may share it with other unauthorized individuals.

Mitigation: The VA provides Windows and Oracle access controls along with the following security controls: Audit and Accountability, Awareness Training, Security Assessment and Authorization, Incident Response, Personnel Security, and Identification and Authentication.
· All personnel with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior Training annually.
· The RES adheres to all information security requirements instituted by the VA Office of Information Technology (OIT).
· Information is shared in accordance with VA Handbook 6500.

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***
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.

Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk: Not Applicable (N/A) Not Applicable (N/A)

Mitigation: Not Applicable (N/A)

Section 6. Notice

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

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

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

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

The Department of Veterans Affairs provides public notice that the system does notice is provided in 2 ways: 1. The System of Record Notice (SORN): a. 58VA21/22/28 86 FR 61858: exist. This SOR Name: Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records VA 2. This Privacy Impact Assessment (PIA) also se eGovernment Act of 2002, Pub.L. 107 rves as notice of the WINRS As required by the 347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through other means."

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

Notice is provided to users as a splash screen prior to accessing the system: This U.S government system is intended to be used by authorized VA network users for viewing and retrieving information only, except as otherwise explicitly authorized. VA information resides on and transmits through computer systems and networks funded by VA. All use is considered to be with an understanding and acceptance that there is no reasonable expectation of privacy for any data or transmissions on Government Intranet or Extranet (non-public) networks or systems. All transactions that occur on this system and all data transmitted through this system are subject to review and action including (but not limited to) monitoring, recording, retrieving, copying, auditing, inspecting, investigating, restricting access, blocking, tracking, disclosing to authorized personnel, or any other authorized actions by all authorized VA and law enforcement personnel. All use of this system constitutes understanding and unconditional acceptance of these terms.

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

The notice above has provided sufficient notice to users. No issues have been raised with this language for as long as it has been part of the legacy system. Users cannot access the system without acknowledging the privacy notice.

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 have the right to decline providing information to VA personnel. However, failure to provide information may result in denial of access to the health care system. Veterans and their family or guardian (spouse, children, parents, grandparents, etc.) may not decline or request their information not be included as part to determine eligibility and entitlement for VA compensation and pension benefits and designate a guardian to manage the VA compensation and pension benefits.

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

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

While individuals may have the ability to consent to various uses of their information at the VA, they are not required to consent to the use of their information as part to determine eligibility and entitlement for VA compensation and pension benefits proceeding. The Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

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. (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:

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

<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? Yes

What procedures are in place to ensure that information is used only for the purpose articulated in the notice?

This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.
Follow the format below:

Privacy Risk: There is a risk that members of the public may not know that the WINRS application exists within the Department of Veterans Affairs.

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

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

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.***

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). Not Applicable.

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.

Individuals wishing to obtain more information about access, redress and record correction of Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records should contact the Department of Veteran's Affairs regional as directed in the System of Record Notice (SORN) "VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA"58VA21/22/28 86 FR 61858. This SORN can be found online at: https://department.va.gov/privacy/

https://department.va.gov/privacy/https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

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

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

Individuals wishing to obtain more information about access, redress and record correction of Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records should contact the Department of Veteran's Affairs regional office as directed in the System of Record Notice (SORN) "VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA" 58VA21/22/28 86 FR 61858.
This SORN can be found online at:
https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Individuals seeking information regarding access to and contesting of VA records may write, call or visit the nearest VA regional office. Address locations are listed in VA Appendix 1, as directed in the System of Record Notice (SORN) "VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA" 58VA21/22/28 86 FR 61858.
This SORN can be found online at: https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

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.

Individuals seeking information regarding access to and contesting of VA records may write, call or visit the nearest VA regional office. Address locations are listed in VA Appendix 1, as directed in the System of Record Notice (SORN) "VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA" 58VA21/22/28 86 FR 61858. This SORN can be found online at: https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

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? Yes

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? Yes

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? Yes
This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk: There is a risk that individuals may seek to access or redress records about them held by the VA Office and become frustrated with the results of their attempt.

Mitigation: By publishing this PIA and the applicable SORN, the VA makes the public aware of the unique status of applications and evidence files, such as those stored on the Virtual VA platform. Furthermore, this document and the SORN provide the point of contact for members of the public who have questions or concerns about applications and evidence files.

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.

User accounts and roles are granted at the local Regional Office level for the minimum access necessary to complete job functions. For individual in VA Central Office, individuals may be granted access by national system administrators after the request have been confirmed and vetted by the user's supervisor. Additionally, accounts are disabled after 90 days of inactivity.

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?

N/A. No users outside of VA will be granted access to RES.

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.

Per VA Directive and Handbook 6330, every 5 years the Office of Information Technology (OIT) develops, disseminates, and reviews/updates a formal, documented policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; along with formal, documented procedures to facilitate the implementation of the control policy and associated controls.
OIT documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and retains individual training records for 7 years. This documentation and monitoring is performed through the use of TMS. Users of VA/VBA information systems gain access through an EO LAN control domain. The EO LAN personnel use Group Policy Objects (GPO) to manage accounts. A GPO is a set of rules which control the working environment of user accounts and computer accounts. The GPO provides the centralized management and configuration of operating systems, applications, and users' settings in an Active Directory environment. The GPO restricts certain actions that may pose potential security risks.

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.

OI&T provides basic security awareness training to all information system users (including managers, senior executives, and contractors) of VA information systems or VA sensitive information as part of initial training for new users, when required by system changes and annually thereafter.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VA's 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.

8.4 Has Authorization and Accreditation (A&A) been completed for the system? No

8.4a If Yes, provide:

1. *The Security Plan Status:* To Be Determined (TBD)
2. *The System Security Plan Status Date:* To Be Determined (TBD)
3. *The Authorization Status:* To Be Determined (TBD)
4. *The Authorization Date:* To Be Determined (TBD)
5. *The Authorization Termination Date:* To Be Determined (TBD)
6. *The Risk Review Completion Date:* To Be Determined (TBD)
7. *The FIPS 199 classification of the system MODERATE.*

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

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

The Readiness and Employment System is a new system and yet to receive ATO. The Initial Operating Capability (IOC) is 03/31/2024

Section 9 – Technology Usage

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

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

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

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

The system uses VA Enterprise Cloud (VAEC), Amazon Web Services (AWS), Government Cloud.

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.*

Not Applicable (N/A)

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

N/A

9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

N/A

9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).

N/A

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

ID	Privacy Controls
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information

ID	Privacy Controls
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.

RENU ROY 349706

Digitally signed by RENU ROY 349706
Date: 2023.10.23 09:58:54 -04'00'

Privacy Officer, Renu Roy

ANDREW VILAILACK

Digitally signed by ANDREW VILAILACK
Date: 2023.10.20 09:23:39 -04'00'

Information System Security Officer, Andrew Vilailack

ROBERT CERVANTES

Digitally signed by ROBERT CERVANTES
Date: 2023.10.20 08:46:16 -04'00'

Information System Owner, Robert M. Cervantes

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://department.va.gov/privacy/
58VA21/22/28 86 FR 61858: SORN Name: 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