



Privacy Impact Assessment for the VA IT System called:

**VBA Data Warehouse
Veterans Benefits Administration
Insurance Products Division Service,
Veterans Benefits
eMASS ID # 127**

Date PIA submitted for review:

12/4/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Marvis Harvey	Marvis.harvey@va.gov	202-461-8401
Information System Security Officer (ISSO)	Dan Dressler	daniel.dressler@va.gov	775-624-4267
Information System Owner	Jami Shofner	jami.shofner@va.gov	512-326-6415

Abstract

The abstract provides the simplest explanation for “what does the system do for VA?”.

VBA Data Management Warehouse is the central repository of all benefits related data, receiving data input from multiple VA data sources, and providing reporting, analysis, and payment data to various organizations throughout the VA and both the Executive and Legislative branches.

Overview

The overview is the most important section of the Privacy Impact Assessment (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. What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?*

The Veterans Benefits Administration (VBA) Data Warehouse (VD2) application is developed and managed by the Enterprise Data Warehouse (EDW) organization within the Office of Performance Analysis and Integrity (PA&I). The data warehouse component of the VD2 application is commonly called the Enterprise Data Warehouse (EDW) and that term will be used for the remainder of this PIA.

The EDW serves as the VBA principal data warehouse and business intelligence (BI) tool for performance, business process, and financial management. As such, the EDW plays a key role in supporting the VBA mission to provide benefits and services to Veterans and their families in a responsive, timely, and compassionate manner. The EDW also satisfies demands for strategic, operational, and Adhoc information from its stakeholders in VBA executive management, Congress, business lines, and other Federal agencies (e.g., Government Accountability Office (GAO) or Department of Defense (DOD)). The EDW also provides self-service reports capability to VBA regional offices day to day operational and workload performance.

The EDW was established to maintain a centralized view of the VBA activities and centralized storage and access to the data needed to perform those activities. The EDW ensures a consistent representation of stored information that is identified and shared among applications to establish a more efficient and consistent approach to facilitating communication between business users.

The centralized collecting and reporting supplied by the EDW provides the following capabilities:

- Centralized collection, storage, review and analysis, and report generation of Veteran and VA information.
- Manage Veteran and VA information, from a headquarters perspective.
- Manage and review information to improve the integrity of crucial Veteran benefits programs.
- Make timely decisions to improve and positively affect the benefit programs managed by the lines of business.
- Centralized information increases the VBA ability to monitor workloads, check the status of cases, and prioritize and allocate appropriate resource levels to Regional Offices.

- The business intelligence program enables the VBA to provide timely and accurate reports to internal and external veteran stakeholders. Stakeholders may include VA organizations, Veteran Service Organizations, Congress, and the Department of Defense.
- Centralized information provides consistent reports instead of disparate messages presented from various VBA organizations.
- Centralized information allows VBA to assess Administration-wide any potential integrity flaws and shortcomings.

The major technical advantage of the EDW is the use of a relational database that eliminates data redundancy and establishes a dynamic reporting infrastructure.

According to the VBA Annual Benefit Report for 2013, more than 4 million Veterans that were serviced that year. To meet the demand for information regarding these services provided, the EDW retained the information associated with the request for service and the administration of these services of almost every era of U.S. history. This data is collected and made available for use by all VBA Regional Offices, VACO and other VA offices. Additionally, the data is used to support thousands of requests for data analysis and reporting from the EDW quarterly.

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 EDW. VA gathers this data to support the mission objectives enabling the VA to administer statutory benefits programs to Veterans, Service members, reservists, their spouses and surviving spouses. The completion of this PIA will not cause changes to business processes or changes in technology. Currently, EDW does not use cloud technology.

B. Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.

VA Owned and VA Operated

2. Information Collection and Sharing

C. Indicate the expected number of individuals whose information is stored in the system and include a brief description of the typical client or affected individual?

Number of unique records is 95,000

Check if Applicable	Demographic of individuals
<input checked="" type="checkbox"/>	Veterans or Dependents
<input checked="" type="checkbox"/>	VA Employees
<input type="checkbox"/>	Clinical Trainees
<input type="checkbox"/>	VA Contractors
<input type="checkbox"/>	Members of the Public/Individuals
<input type="checkbox"/>	Volunteers

D. What is a general description of the information in the IT system and the purpose for collecting this information?

VBA Data Warehouse (VD2) is resident in an Oracle M8 SuperCluster server located at AITC. VD2 was established to maintain centralized storage with a common view of all the Veterans Benefits Administration's activities and to provide a reporting infrastructure, which serves processed data from the warehouse data store to thousands of users VBA-wide via a Web interface. The DW ensures a consistent representation of stored information that is identified and shared among other VBA applications to establish a more efficient and consistent approach to facilitating communication between business users. It also eliminates data redundancy.

E. What information sharing is conducted by the IT system? A general description of the modules and components, where relevant, and their functions.

This is to provide data for determination and awarding of benefits and provide historical archive of that information.

F. Are the modules/subsystems only applicable if information is shared?

No. This is also a historical archive.

G. Is the system operated in more than one site to include primary and secondary 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?

No

3. *Legal Authority and System of Record Notices (SORN)*

H. *What is the citation of the legal authority?*

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code, Section 501

<https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01516.pdf>

45VA21 Veterans Assistance Discharge System-VA 58VA21/22/28 Compensation Pension, Education and Rehabilitation Records-VA.

H. *What is the SORN?*

[https://www.oprm.va.gov/docs/SORN/Current SORN List 05 30 2023.pdf](https://www.oprm.va.gov/docs/SORN/Current%20SORN%20List%2005%2030%202023.pdf)

<https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01516.pdf>

45VA21 Veterans Assistance Discharge System-VA 58VA21/22/28 Compensation Pension, Education and Rehabilitation Records-VA.

J. *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval.*

No

4. *System Changes*

K. *Will the business processes change due to the information collection and sharing?*

Yes

No

if yes, <<ADD ANSWER HERE>>

L. *Will the technology changes impact information collection and sharing?*

Yes

No

if yes, <<ADD ANSWER HERE>>

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 Information 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 (II), 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. It must also match the information provided in question 3.4 of the PTA.

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:

- | | | |
|---|--|---|
| <input checked="" type="checkbox"/> Name | <input checked="" type="checkbox"/> Health Insurance Beneficiary Numbers | <input checked="" type="checkbox"/> Military History/Service Connection |
| <input checked="" type="checkbox"/> Full Social Security Number | Account Numbers | <input checked="" type="checkbox"/> Next of Kin |
| <input type="checkbox"/> Partial Social Security Number | <input type="checkbox"/> Certificate/License numbers ¹ | <input checked="" type="checkbox"/> Date of Death |
| <input checked="" type="checkbox"/> Date of Birth | <input type="checkbox"/> Vehicle License Plate Number | <input type="checkbox"/> Business Email Address |
| <input type="checkbox"/> Mother's Maiden Name | <input type="checkbox"/> Internet Protocol (IP) Address Numbers | <input type="checkbox"/> Electronic Data Interchange Personal Identifier (EDIPI) <input type="checkbox"/> |
| <input checked="" type="checkbox"/> Personal Mailing Address | <input checked="" type="checkbox"/> Medications | Other Data Elements (list below) |
| <input checked="" type="checkbox"/> Personal Phone Number(s) | <input checked="" type="checkbox"/> Medical Records | |
| <input type="checkbox"/> Personal Fax Number | <input type="checkbox"/> Race/Ethnicity | |
| <input checked="" type="checkbox"/> Personal Email Address | <input type="checkbox"/> Tax Identification Number | |
| <input type="checkbox"/> Emergency Contact Information (Name, Phone Number, etc. of a different individual) | <input type="checkbox"/> Medical Record Number | |
| <input checked="" type="checkbox"/> Financial Information | <input checked="" type="checkbox"/> Gender/Sex | |
| | <input type="checkbox"/> Integrated Control Number (ICN) | |

Other PII/PHI data elements: Payee number and type of benefits

1.2 List 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?

¹ *Specify type of Certificate or License Number (e.g., Occupational, Education, Medical)

The sources of data collection for the EDW are from the VBA applications' databases (source systems). Data is extracted nightly from the application databases by batch software processes which read data from the databases, normalize the data, and then write the data to the EDW. Data from applications include the Compensation & Pension Master Record (CPMR), Vocational Rehabilitation and Employment (VRE) files, Loan Guaranty (LGY) files, and Employee Personnel data files from the VBA central data repository.

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.

The system does not pull data from non-governmental sources.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?

Yes, generates reports utilized by VBA regional offices.

1.3 Methods of information collection

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?

EDW Data/information is collected by secured transmission of data from VA Corporate data warehouse, other VBA application system, external government, and non-government agency systems. This data is then integrated into the EDW utilizing batch processes to normalize the data. Information is also collected by the Veteran or authorized individuals via on-line VA form applications.

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

The system does not get information from forms.

1.4 Information checks for accuracy, and how often will it be checked.

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

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

The system does not get information from forms to store.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

The system relies on entities within the VBA to verify information collected.

1.5 Identify the specific legal authorities, arrangements, and agreements that 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 EDW 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.

Public Law 104-134 (April 26, 1996) requires that any person doing business with the Federal Government furnish a Social Security Number or tax identification number. This is an amendment to title 31, Section 7701.

The Secretary of Veterans Affairs established these guidelines pursuant to the authorities in and requirements of Title 38, United States Code, section 8111 (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. 51104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51535), titled "Agency Agreements," also known as the "Economy Act." These guidelines assist in the implementation of these statutes.

https://www.oprm.va.gov/docs/SORN/Current_SORN_List_05_30_2023.pdf

<https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01516.pdf>

45VA21 Veterans Assistance Discharge System-VA 58VA21/22/28 Compensation Pension, Education and Rehabilitation Records-VA.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

Principle of Minimization: The information is directly relevant and necessary to accomplish the specific purposes of the program.

Principle of Individual Participation: The program, to the extent possible and practical, collects information directly from the individual.

Principle of Data Quality and Integrity: VA policies and procedures must ensure that personally identifiable information is accurate, complete, and current.
This 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 EDW components adhere 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.
- VA Regional Loan Center (RLC) staff, and VBA VACO Monitoring Unit staff also conduct audits of the lenders loan files (which included auditing funding fee information) as part of ongoing lender and RLC quality audits.

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 that 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.

PII/PHI Data Element	Internal Use	External Use
Names,	Storage of benefits information	Determination of benefits
Full Social Security	Storage of benefits information	Determination of benefits
Date of Birth	Storage of benefits information	Determination of benefits
Personal Mailing Address	Storage of benefits information	Determination of benefits
Personal Phone Number(s)	Storage of benefits information	Determination of benefits
Financial Information	Storage of benefits information	Determination of benefits
Personal Email Address	Storage of benefits information	Determination of benefits
Financial Information	Storage of benefits information	Determination of benefits

Health Insurance Beneficiary Numbers	Storage of benefits information	Determination of benefits
Medications	Storage of benefits information	Determination of benefits
Medical Records	Storage of benefits information	Determination of benefits
Gender/Sex	Storage of benefits information	Determination of benefits

2.2 Describe the types of tools 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?

The system does not perform this function but rather utilizes existing data for report

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 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. 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.

The EDW through the nightly batch process receives any new or updated data/information.

2.3 How the information in the system is 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?

Data in Transit - All data in transit is protected by encryption secure shell or secure copy.

Data at Rest - Encrypted at the hardware level and protected via two factor authentications.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? (refer to PTA question 3.8).

Encrypted at the hardware level and protected via two factor authentications. Data in Transit - All data in transit is protected by encryption secure shell or secure copy. Data at Rest - Encrypted at the hardware level and protected via two factor authentications.

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

Encrypted at the hardware level and protected via two factor authentications. Data in Transit - All data in transit is protected by encryption secure shell or secure copy. Data at Rest - Encrypted at the hardware level and protected via two factor authentications.

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?

Accounts are approved, created and granted using the Access Request through ePAAS, the form gathers appropriate level of approval for requested access. System Administrators manage all accounts using this form and a Service Desk Manager (SDM) ticket. This procedure is documented in the system security plan as follows:

Application:

VBA information systems employ automated mechanisms to support information systems account management. The use of automated mechanisms ensures that account creation, modification, disabling, and termination are auditable and that appropriate personnel are notified of these occurrences. VBA information systems utilize Group Policy Objects (GPO) to manage accounts. GPO is a set of rules which control the working environment of user accounts and computer accounts. Group policy Objects provides the centralized management and configuration of operating systems, applications and users' settings in an Active Directory environment. Group policy objects restrict certain actions that may pose potential security risks. Infrastructure Operations (IO) manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts for hardware components (application server, web server, database server, policy server) that reside at the IO. IO does not establish access control requirements for users. IO reviews information system accounts every 90 days.

Windows System Administration:

Accounts are created manually. Manual monthly reports are done to identify inactive accounts. Accounts are manually disabled if the account has not been active for over 90 days.

Linux System Administration:

Accounts are created manually. A cron job checks for accounts that have been inactive for 90 days and locks those accounts.

As an account approaches expiration, notifications are sent by the cron job to users. The cron job creates a ticket for system admins to remove an account after it has been inactive for over 180 days.

Solaris & HP-UX System Administrations:

Accounts are created manually. A script runs daily looking for accounts that have been inactive over 90 days. For any account that is found, a notification is sent out for manual removal. Oracle Application Server, Database Server and OBIEE include features that are designed to permit only authorized access to or within the system, to restrict users to authorized transactions and functions, and to detect unauthorized activities. Only authenticated user IDs are permitted to have access to VD2 and its interfaces. Austin CFD accounts are enforced at the database level. User access has been restricted (least privilege) to data files and processing capability (i.e., read, write, execute, delete) to the minimum necessary to perform the job.

- a) Account types individual accounts (admins only), global groups and service accounts. The guest account is disabled and there is no anonymous access. There should be no local accounts; the exception to this is the Technical Security scanning account for DMZ servers.
- b) Group accounts are created through the VA ePAAS processes.
- c) VA ePAAS are used when creating accounts and granting appropriate access.
- d) VA ePAAS are used to gather appropriate approvals for access.
- e) Infrastructure admins manage all active directory accounts. Accounts are provisioned only upon a VA ePAAS or appropriate USD ticket.
- f) Guest/anonymous and temporary accounts are not allowed.
- g) Temporary accounts and “need-to-know” changes aren’t applicable. For terminations and transfers, the VA ePAAS process makes sure all access changes are handled.
- h) Account deletions are done SDM ticket or VA ePAAS.
- i) The VA ePAAS process covers expected usage, necessary access, etc.
- j) Account reviews are not performed.

Linux:

- a) Guest/anonymous and temporary accounts don’t exist. There are individual accounts, service accounts for monitoring and applications (WebLogic, Patrol, Nagios and Oracle) and group accounts users can run commands as.
- b) Group accounts are built in as part of the install routine; there are open VA ePAAS tickets for those accounts. Individual users are later defined as a member of the group.
- c) VA ePAAS are used when creating accounts and granting appropriate access.
- d) VA ePAAS are used to gather appropriate approvals for access.
- e) System Administrators manage all accounts through sudo. They provision accounts only upon a VA ePAAS or appropriate USD ticket.
- f) Guest/anonymous and temporary accounts are not allowed.
- g) Temporary accounts and “need-to-know” changes aren’t applicable. For terminations and transfers, the ePAAS process makes sure all access changes are handled
- h) Account deletions may come by USD ticket if they are inactive for 180 days or VA ePAAS.
- i) The VA ePAAS process covers expected usage, necessary access, etc.
- j) Accounts are not reviewed by system administrators.

Solaris:

- a) Guest/anonymous and temporary accounts don’t exist. Yes the rest of the accounts consist of individual, group, system and application.

- b) Service accounts are managed by group membership; only group members can “su” to service accounts.
- c) VA ePAAS are used when creating accounts and granting appropriate access.
- d) VA ePAAS are used to gather appropriate approvals for access.
- e) System admins manage all accounts. They provision accounts only upon a appropriate USD ticket.
- f) Guest/anonymous and temporary accounts are not allowed.
- g) Temporary accounts and “need-to-know” changes aren’t applicable. For terminations and transfers, the VA ePAAS process makes sure all access changes are handled.
- h) Account deletions may come by SDM ticket.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented? How are the documented, i.e. Policy, SOP, other. And where is this documentation located?

The system documents how it implements its security controls in the Standard Operating Procedures (SOPs)

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 as identified in eMASS?

Information System Owner (ISO)

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 Address
- Financial Account Information
- Service Number
- Rank
- Total amount of active service

- Branch of service
- Character of service
- Pay grade
- Assigned separation reason
- Service period
- Birth certificates
- Marriage licenses
- Discharged with disability status
- Reenlisted
- Received a Purple Heart or other Military decoration

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 <https://www.archives.gov/records-mgmt/grs?> This question is related to privacy control DM-2, Data Retention and Disposal.*

Data from source systems is constantly updated on a nightly basis. When new source system files are available, they are transferred to the warehouse. Old files are saved using backup tapes.

The EDW is non-volatile, so the data is never over-written or deleted--after the data is committed; the data is static, read-only, and retained for future reporting. Thus, data is retained indefinitely.

The EDW is designed and built to answer virtually any question that requires data to answer it. Many questions surround the issue of trending or a comparison of data from one period of time to another. In order to answer any question, data must be collected and stored in the EDW indefinitely. Depending on the application within the data warehouse, old data (as defined in business rules) can be archived to tape (or other fixed media), but can be restored to the data warehouse within one day of a request to do so.

The EDW is a working repository of electronically copied business line data. It is kept as needed per RCS, VB-1 Part II, Section 1-6.2 (Non-record sensitive material extracted from a system of storage). Destroy when no longer needed.

3.3 The retention schedule 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. Please work with the system VA Records Officer to answer these questions.

This question is related to privacy control DM-2, Data Retention and Disposal.

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

VBA Records Management, Records Control Schedule VB-1, Part 1, Section VII as authorized by NARA.

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

VB-1 Part II can be found at:

https://www.benefits.va.gov/WARMS/docs/regs/RCS_II.doc and

<https://www.benefits.va.gov/WARMS/21guides.asp>

Additional information can be found at: https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/departments-of-veterans-affairs/rg-0015/n1-015-90-001_sf115.pdf

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 in accordance with VA Directive 6371. 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.

The EDW IT deployments testing are done with internal systems and users have access and need for data through VA policy. Research purposes and training; information is redacted and/or sent per VA FOIA, the business lines are responsible.

EDW has environments; Development, Pre-Production, Test and Production, all are under EDW system accreditation boundary which means they have the same security protocol as production data.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System Privacy Officer (PO) 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: The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.

Principle of Data Quality and Integrity: The PIA should describe 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, EDW retains 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.

Mitigation: Redaction of some information is required by law which reduces the risk 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 users must be authenticated on the VA network, have a PIV card and be approved by VA for access.

Data is received and sent using encrypted methods.

The EDW is a working repository of electronically copied business line data. It is kept as needed per RCS, VB-1 Part II, Section 1-6.2 (Non-record sensitive material extracted from a system of storage). Destroy when no longer needed.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

PII Mapping of Components

4.1a VBA Data Warehouse consists of 6 key components (servers/databases/instances/applications/software/application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect PII. The type of

PII collected by VBA Data Warehouse 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 server names in the table. The first table of 3.9a in the PTA should be used to answer this question.

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	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
VBAEDW1 VBAODS1	Yes	Yes	Names, addresses, emails, health information, financial information, SSN, payee number and type of benefits	Centralized collection, storage, review and analysis, and report generation of veteran and VA information. Manage and review information to improve the integrity of crucial veteran benefits programs. Make timely decisions to improve and positively affect the benefit programs managed by the lines of business. Centralized information increases the VBA ability to monitor	Oracle Web Reports (with option to download data in xls and pdf)

				workloads, check the status of cases, and prioritize and allocate appropriate resource levels to Regional Offices. The business intelligence program enables the VBA to provide timely and accurate reports to internal and external veteran stakeholders. Stakeholders may include VA organizations, Veteran Service Organizations, Congress, and the Department of Defense	
EDWCERT ODSUAT1	Yes	Yes	Names, addresses, emails, health information, financial information, SSN, payee number and type of benefits	Centralized collection, storage, review and analysis, and report generation of veteran and VA information. Manage and review information to improve the integrity of crucial veteran benefits	Only authorized users can access information. Authorized users are VA employees or Contractors. Privacy and security controls

				<p>programs. Make timely decisions to improve and positively affect the benefit programs managed by the lines of business.</p>	
EDWDEV1 ODSDEV1	Yes	Yes	Names, addresses, emails, health information, financial information, SSN, payee number and type of benefits	<p>Centralized collection, storage, review and analysis, and report generation of veteran and VA information. Manage and review information to improve the integrity of crucial veteran benefits programs. Make timely decisions to improve and positively affect the benefit programs managed by the lines of business. Centralized information increases the VBA ability to monitor workloads, check the status of cases, and prioritize and allocate</p>	<p>Only authorized users can access information. Authorized users are VA employees or Contractors. Privacy and security controls</p>

				<p>appropriate resource levels to Regional Offices. The business intelligence program enables the VBA to provide timely and accurate reports to internal and external veteran stakeholders. Stakeholders may include VA organizations, Veteran Service Organizations, Congress, and the Department of Defense.</p>	
EDWTST1 ODSTEST1	Yes	Yes	Names, addresses, emails, health information, financial information, SSN, payee number and type of benefits	Centralized collection, storage, review and analysis, and report generation of veteran and VA information. Manage and review information to improve the integrity of crucial veteran benefits programs. Make timely decisions to improve and	Only authorized users can access information. Authorized users are VA employees or Contractors. Privacy and security controls

				<p>positively affect the benefit programs managed by the lines of business. Centralized information increases the VBA ability to monitor workloads, check the status of cases, and prioritize and allocate appropriate resource levels to Regional Offices. The business intelligence program enables the VBA to provide timely and accurate reports to internal and external veteran stakeholders. Stakeholders may include VA organizations, Veteran Service organizations, Congress, and the Department of Defense.</p>	
--	--	--	--	--	--

4.1b List internal organizations information is shared/received/transmitted, the information shared/received/transmitted, and the purpose, and how the information is transmitted.

NOTE: Question 3.9b (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

<i>IT system and/or Program office. Information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List PII/PHI data elements shared/received/transmitted.</i>	<i>Describe the method of transmittal</i>
Veterans Benefit Administration (VBA)	Centralized collection, storage, review and analysis, and report generation of veteran and VA information. Manage and review information to improve the integrity of crucial veteran benefits programs. Make timely decisions to improve and positively affect the benefit programs managed by the lines of business. Centralized information increases the VBA ability to monitor	Names, addresses, emails, health information, financial information, SSN, payee number and type of benefits	Oracle Web Reports (with option to download data in xls and pdf)

<i>IT system and/or Program office. Information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List PII/PHI data elements shared/received/transmitted.</i>	<i>Describe the method of transmittal</i>
	workloads, check the status of cases, and prioritize and allocate appropriate resource levels to Regional Offices. The business intelligence program enables the VBA to provide timely and accurate reports to internal and external veteran stakeholders. Stakeholders may include VA organizations, Veteran Service Organizations, Congress, and the Department of Defense		
Compensation & Pension Master Record (CPMR)	Centralized collection, storage, review and analysis, and report generation of veteran and VA information. Manage and review information to improve the integrity of crucial veteran benefits programs. Make timely decisions to improve and positively affect the benefit programs managed by the lines of business. Centralized information increases the VBA ability to monitor workloads, check the status of cases, and prioritize and allocate appropriate resource levels to Regional Offices. The business	Names, addresses, emails, health information, financial information, SSN, payee number and type of benefits	Oracle Web Reports (with option to download data in xls and pdf)

<i>IT system and/or Program office. Information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List PII/PHI data elements shared/received/transmitted.</i>	<i>Describe the method of transmittal</i>
	intelligence program enables the VBA to provide timely and accurate reports to internal and external veteran stakeholders. Stakeholders may include VA organizations, Veteran Service Organizations, Congress, and the Department of Defense		
Loan Guaranty LGY	Centralized collection, storage, review and analysis, and report generation of veteran and VA information. Manage and review information to improve the integrity of crucial veteran benefits programs. Make timely decisions to improve and positively affect the benefit programs managed by the lines of business. Centralized information increases the VBA ability to monitor workloads, check the status of cases, and prioritize and allocate appropriate resource levels to Regional Offices. The business intelligence program enables the VBA to provide timely and accurate reports to internal and external veteran stakeholders.	Names, addresses, emails, health information, financial information, SSN, payee number and type of benefits	Oracle Web Reports (with option to download data in xls and pdf)

<i>IT system and/or Program office. Information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List PII/PHI data elements shared/received/transmitted.</i>	<i>Describe the method of transmittal</i>
	Stakeholders may include VA organizations, Veteran Service Organizations, Congress, and the Department of Defense		
Human Resources (HR)	<p>Centralized collection, storage, review and analysis, and report generation of veteran and VA information. Manage and review information to improve the integrity of crucial veteran benefits programs. Make timely decisions to improve and positively affect the benefit programs managed by the lines of business.</p> <p>Centralized information increases the VBA ability to monitor workloads, check the status of cases, and prioritize and allocate appropriate resource levels to Regional Offices. The business intelligence program enables the VBA to provide timely and accurate reports to internal and external veteran stakeholders. Stakeholders may include VA organizations, Veteran Service Organizations, Congress, and the Department of Defense</p>	Names, addresses, emails, health information, financial information, SSN, payee number and type of benefits	Oracle Web Reports (with option to download data in xls and pdf)

<i>IT system and/or Program office. Information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List PII/PHI data elements shared/received/transmitted.</i>	<i>Describe the method of transmittal</i>
Education Service (EDU)	<p>Centralized collection, storage, review and analysis, and report generation of veteran and VA information. Manage and review information to improve the integrity of crucial veteran benefits programs. Make timely decisions to improve and positively affect the benefit programs managed by the lines of business. Centralized information increases the VBA ability to monitor workloads, check the status of cases, and prioritize and allocate appropriate resource levels to Regional Offices. The business intelligence program enables the VBA to provide timely and accurate reports to internal and external veteran stakeholders. Stakeholders may include VA organizations, Veteran Service Organizations, Congress, and the Department of Defense</p>	Names, addresses, emails, health information, financial information, SSN, payee number and type of benefits	Oracle Web Reports (with option to download data in xls and pdf)
Vocational, Rehabilitation & Employment (VRE)	<p>Centralized collection, storage, review and analysis, and report generation of veteran and VA information. Manage and review</p>	Names, addresses, emails, health information, financial information, SSN, payee number and type of benefits	Oracle Web Reports (with option to download data in xls and pdf)

<i>IT system and/or Program office. Information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List PII/PHI data elements shared/received/transmitted.</i>	<i>Describe the method of transmittal</i>
	<p>information to improve the integrity of crucial veteran benefits programs. Make timely decisions to improve and positively affect the benefit programs managed by the lines of business. Centralized information increases the VBA ability to monitor workloads, check the status of cases, and prioritize and allocate appropriate resource levels to Regional Offices. The business intelligence program enables the VBA to provide timely and accurate reports to internal and external veteran stakeholders. Stakeholders may include VA organizations, Veteran Service Organizations, Congress, and the Department of Defense</p>		

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the VA network 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 in this section.).

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

Follow the format below:

Privacy Risk: There is a risk that EDW 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 annually.
- The EDW 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 List the external organizations (outside VA) that information shared/received, and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.

The sharing of information outside the agency must be compatible with the original collection. The sharing must be covered by an appropriate routine use in a SORN. If not covered, 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

<i>List IT System or External Program Office information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted)</i>	<i>List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>
N/A - The EDW information is not shared outside the VA boundary	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.

If no External Sharing listed on the table above, (State there is no external sharing in both the risk and mitigation fields).

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: EDW data is not shared outside of the VA boundary.

Mitigation: EDW data is not shared outside of the VA boundary.

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 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms, notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.

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 Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.

Public notice is provided in two ways:

1. https://www.oprm.va.gov/docs/SORN/Current_SORN_List_05_30_2023.pdf
<https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01516.pdf>

45VA21 Veterans Assistance Discharge System-VA 58VA21/22/28 Compensation Pension, Education and Rehabilitation Records-VA.

2. This Privacy Impact Assessment (PIA) also serves as notice of the EDW. As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs “after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available

VBA also provides notice on the authority for collecting PII and choices regarding the PII at the point of collection. The Privacy Act Statements on the paper and electronic forms explain whether data collection is mandatory or voluntary and explains the consequences of not providing the information when data collection is voluntary.

6.1b If notice was not provided, explain why.

VBA provides notice for collecting PII.

6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.

VBA also provides notice on the authority for collecting PII and choices regarding the PII at the point of collection.

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.

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

The Privacy Act Statements on the paper and electronic forms explain whether data collection is mandatory or voluntary and explains the consequences of not providing the information when data collection is voluntary.

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.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

Principle of Transparency: *This is referring to sufficient notice provided to the individual.*

Principle of Use Limitation: *The information used only for the purpose for which notice was provided either directly to the individual or through a public notice. The procedures in place must 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 EDW 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 this Privacy Impact Assessment (PIA) and the System of Record Notice(s).

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 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 [VA Public Access Link-Home \(efoia-host.com\)](http://efoia-host.com) to obtain information about FOIA points of contact and information about agency FOIA processes.

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. This SORN can be found online at: [VA Public Access Link-Home http://www.gpo.gov/fdsys/pkg/FR-2012-07-19/pdf/2012-17507.pdf](http://www.gpo.gov/fdsys/pkg/FR-2012-07-19/pdf/2012-17507.pdf)

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

The system is included in the access provisions of the Privacy act

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

The system is not a Privacy Act system and does not have a procedure and regulation in place that covers individual gaining access to their information.

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 as directed in the System of Record Notice (SORN) "VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment

Records – VA” 58VA21/22/28,.This SORN can be found online at:
<http://www.gpo.gov/fdsys/pkg/FR-2012-07-19/pdf/2012-17507.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 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,.This SORN can be found online at: <http://www.gpo.gov/fdsys/pkg/FR-2012-07-19/pdf/2012-17507.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 ensure data accuracy.

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 as directed in the System of Record Notice (SORN) “VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA” 58VA21/22/28,.This SORN can be found online at:

<http://www.gpo.gov/fdsys/pkg/FR-2012-07-19/pdf/2012-17507.pdf>

“Veterans and Beneficiaries Identification Records Location Subsystem” -VA-38VA21. This SORN can be found online at: <https://www.oprm.va.gov/docs/sorn/SORN38VA21.docx>

“Veterans Assistance Discharge System”- VA45VA21. This SORN can be found online at:

<https://www.gpo.gov/fdsys/pkg/FR-2010-10-06/pdf/2010-25233.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 Privacy Officer (PO) to complete all Privacy Risk questions in this section).

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

Principle of Individual Participation: *The individual must be provided with the ability to find out whether a project maintains a record relating to them.*

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

Principle of Individual Participation: *The mechanism by which an individual is able to prevent information about them obtained for one purpose from being used for other purposes without their knowledge.*

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 their information within the EDW system/application.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures. (Work with your ISSO to complete this section).

8.1 The procedures in place to determine which users may access the system, must be 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?

Users of VA/VBA information systems gain access through an IO LAN control domain. The IO 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. Accounts are approved using VA ePAAS form with layers for approval and the procedure is documented in the system security plan as follows:

Application:

VBA information systems employ automated mechanisms to support information systems account management. The use of automated mechanisms ensures that account creation, modification, disabling, and termination are auditable and that appropriate personnel are notified of these occurrences. VBA information systems utilize Group Policy Objects (GPO) to manage accounts. GPO is a set of rules which control the working environment of user accounts and computer accounts. Group policy Objects provides the centralized management and configuration of operating Systems, applications and users' settings in an Active Directory environment. Group policy objects restrict certain actions that may pose potential security risks. IO manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts for hardware components (application server, web server, database server, policy server) that reside at the IO. IO does not establish access control requirements for users. IO reviews information system accounts every 90 days.

Windows System Administration:

Accounts are created manually. Manual monthly reports are done to identify inactive accounts. Accounts are manually disabled if the account has not been active for over 90 days.

Linux System Administration:

Accounts are created manually. A cron job checks for accounts that have been inactive for 90 days and locks those accounts.

As an account approaches expiration, notifications are sent by the cron job to users. The cron job creates a ticket for system admins to remove an account after it has been inactive for over 180 days.

Solaris & HP-UX System Administrations:

Accounts are created manually. A script runs daily looking for accounts that have been inactive over 90 days. For any account that is found, a notification is sent out for manual removal.

Oracle Application Server, Database Server and OBIEE include features that are designed to permit only authorized access to or within the system, to restrict users to authorized transactions and functions, and to detect unauthorized activities. Only authenticated user IDs are permitted to have access to VD2 and its interfaces. Austin CFD accounts are enforced at the database level. VBA personnel are granted direct access to Discoverer in email notifications. User access has been restricted (least privilege) to data files and processing capability (i.e., read, write, execute, delete) to the minimum necessary to perform the job.

- a) Account types individual accounts (admins only), global groups and service accounts. The guest account is disabled and there is no anonymous access. There should be no local accounts; the exception to this is the Technical Security scanning account for DMZ servers.
- b) Group accounts are created through VA ePAAS process.
- c) VA ePAAS are used when creating accounts and granting appropriate access.
- d) VA ePAAS are used to gather appropriate approvals for access.
- e) Infrastructure admins manage all active directory accounts. Accounts are provisioned only upon a VA ePAAS or appropriate USD ticket.
- f) Guest/anonymous and temporary accounts are not allowed.
- g) Temporary accounts and “need-to-know” changes aren’t applicable. For terminations and transfers, VA ePAAS process makes sure all access changes are handled.
- h) Account deletions may come by SDM ticket or VA ePAAS.
- i) The VA ePAAS process covers expected usage, necessary access, etc.
- j) Account reviews are not performed.

Linux:

- a) Guest/anonymous and temporary accounts don't exist. There are individual accounts, service accounts for monitoring and applications (WebLogic, Patrol, Nagios and Oracle) and group accounts users can run commands as.
- b) Group accounts are built in as part of the install routine; there are open VA ePAAS tickets for those accounts. Individual users are later defined as a member of the group.
- c) VA ePAAS are used when creating accounts and granting appropriate access.
- d) VA ePAAS are used to gather appropriate approvals for access.
- e) System admins manage all accounts through sudo. They provision accounts only upon a ePAAS or appropriate USD ticket.
- f) Guest/anonymous and temporary accounts are not allowed.
- g) Temporary accounts and "need-to-know" changes aren't applicable. For terminations and transfers, the ePAAS process makes sure all access changes are handled.
- h) Account deletions may come by USD ticket if they are inactive for 180 days or VA ePAAS form.
- i) The VA ePAAS process covers expected usage, necessary access, etc.
- j) Accounts are not reviewed by system administrators.

Solaris:

- a) Guest/anonymous and temporary accounts don't exist. Yes the rest of the accounts consist of individual, group, system and application.
- b) Service accounts are managed by group membership; only group members can "su" to service accounts.
- c) ePAAS's are used when creating accounts and granting appropriate access.
- d) ePAAS's are used to gather appropriate approvals for access.
- e) System admins manage all accounts. They provision accounts only upon a ePAAS or appropriate USD ticket.
- f) Guest/anonymous and temporary accounts are not allowed.
- g) Temporary accounts and "need-to-know" changes aren't applicable. For terminations and transfers, the ePAAS process makes sure all access changes are handled.
- h) Account deletions may come by SDM ticket or ePAAS.

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?

There are no other agencies who can access the system.

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.

User Role - Read

Author Role - Editor

Administrator Role – Administrator

8.2a. Will VA contractors have access to the system and the PII?

VA contractors access the EDW. The EDW development team comprises VA personnel and contractors. Access to the EDW is required by system administrators for day-to-day maintenance of the systems and networks.

8.2b. What involvement will contractors have with the design and maintenance of the system?

The software developers require access for maintenance and development of the EDW software. Review of access to the EDW is performed on a quarterly basis by the ISO and the security engineer. Clearance is required for each person accessing the system. Contracts are reviewed annually by the Contracting Officer's Technical Representative.

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.

8.2c. Does the contractor have a signed confidentiality agreement?

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

8.2d. Does the contractor have an implemented Business Associate Agreement for applicable PHI?

Contractors take the VA Privacy and Information Security Awareness and Rules of Behavior and HIPPA training.

8.2e. Does the contractor have a signed non-Disclosure Agreement in place?

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.

After contractors complete training they are required to sign the Rules of Behavior before granted access the VA environment.

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 VA sensitive information and/or VA 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 re-affirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. HIPPA is part of training. System administrators and elevated privileged users are required to complete additional role-based training.

8.4 The Authorization and Accreditation (A&A) completed for the system.

8.4a If Yes, provide:

1. *The Security Plan Status: Approved*
2. *The System Security Plan Status Date: 6/26/2023*
3. *The Authorization Status: ATO (Authority To Operate)*
4. *The Authorization Date: 8/11/2023*
5. *The Authorization Termination Date: 8/10/2025*
6. *The Risk Review Completion Date: 9/23/2021*
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.***

N/A

Section 9 – Technology Usage

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

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

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMAaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties. (Refer to question 1.8 of the PTA)

N/A

9.2 Does the contract with the Hosting 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 3.3.1 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.

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

9.1 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
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 provided in this Privacy Impact Assessment is true and accurate.

Privacy Officer, Marvis Harvey

Information Systems Security Officer, Dan Dressler

Information Systems Owner, Jami Shofner

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; screen shot of a website collection privacy notice).

HELPFUL LINKS:

[Records Control Schedule 10-1 \(va.gov\)](#)

General Records Schedule

<https://www.archives.gov/records-mgmt/grs.html>

National Archives (Federal Records Management):

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

VA Publications:

<https://www.va.gov/vapubs/>

VA Privacy Service Privacy Hub:

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

Notice of Privacy Practice (NOPP):

VHA Directive 1605.04

[IB 10-163p \(va.gov\)](#)