Privacy Impact Assessment for the VA IT System called:

Enterprise Veterans Self Service Portal (EVSS)

VA Benefits Assistance Service

Date PIA submitted for review:

03/20/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Jean-Claude Wicks	Jean-Claude.Wicks@va.gov	202-502-0084
Information System Security Officer (ISSO)	Joseph Facciolli	Joseph.Facciolli@va.gov	(215) 842-2000 x2012
Information System Owner	Dale Beehler	Dale.Beehler@va.gov	(719) 488-2415

Abstract

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

Enterprise Veterans Self Service Portal (EVSS) will allow a user to access information on available benefits from the VA. VONNAP Direct Connect (EVSS) component of EVSS supports the user by producing a variety of forms for submission to determine eligibility, apply for benefits, view benefits and correct outdated information. EVSS supports a single sign on solution provided by Identity Access Management VA Authentication Federation Infrastructure (IAM VAAFI) to allow users to sign on seamlessly to various portals inside the VA. Users can also access this information via their mobile device. The primary focus for EVSS will be for the Wounded Warrior and Veterans who are eligible to receive benefits.

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.
Enterprise Veterans Self Service Portal (EVSS) and VA Benefits Assistance Service.

B. The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.
EVSS provides a platform for Veterans, as well as eligible spouses and dependents, to manage their VA benefits, claims, and military documents online. A second method of accessibility to EVSS functionality is through Vets.gov. Veteran users are authenticated with Vets.gov prior to being provided access to EVSS.

C. Indicate the ownership or control of the IT system or project.
VA Benefits Assistance Service (BAS)

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.
The Enterprise Veterans Self Service Portal has the potential to be used by all Veterans and dependents (up to 14 million veterans)) registered with the Defense Enrollment Eligibility Reporting System (DEERS).

E. A general description of the information in the IT system and the purpose for collecting this information.
Veterans, beneficiaries, military service members, and other eligible claimants currently use the VONNAP Direct Connect (EVSS) component of EVSS for submitting claims electronically. EVSS provides a Web-based online presence that allows users to browse or search military service-related

and Veteran benefits information. EVSS users are allowed to establish secure accounts with a unique username and password, receive personalized and customized information relevant to them, conduct online transactions related to the application for VBA benefits and services, and to maintain those VBA benefits and services. EVSS allows veterans and beneficiaries the ability to apply for and manage their benefits.

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

Veterans, beneficiaries, military service members, and other eligible claimants currently use the VONNAP Direct Connect (EVSS) component of EVSS for submitting claims electronically. EVSS provides a Web-based online presence that allows users to browse or search military service-related and Veteran benefits information. EVSS users are allowed to establish secure accounts with a unique username and password, receive personalized and customized information relevant to them, conduct online transactions related to the application for VBA benefits and services, and to maintain those VBA benefits and services. Additional verification support is provided by interfacing applications like the Benefits Gateway Service (BGS) and DEERS. Veteran Service Officer (VSO) Representatives may access EVSS on behalf of Veterans for whom they are authorized to represent via the Stakeholder Enterprise Portal (EVSS).

EVSS is designed to use service-oriented architecture (SOA), which allows interfacing with downstream claims processing applications. Beneficiary Identification Locator Subsystem (BIRLS) for assignment of Veteran File Numbers and maintenance of military service information. Chapter 33 (CH33) receives and provides eligibility/entitlement information. Loan Guaranty Service (LGY) provides Veterans with loan information and applications. Master Veteran Index/Person Services Identity Management (MVI/PSM) assigns and maintains unique patient identifiers. My HealtheVet (MHV) provides access to health appointments and prescription refills. Office of the General Council (OCG) verifies Veteran Service Officer (VSO) accreditation. VA DoD Identity Repository (VADIR) provides military service information for Veterans and service members. Veterans Authorizations and Preferences (NVP/VAP) allows the Veteran to control release of health information by forms completion within EVSS. VA Corporate Web Environment (WBT) Benefits Enterprise Platform (BEP) provides a general support system for web-based Veterans Benefits Administration (VBA) business line applications.

Compensation and Pension (C&P) Corporate Applications (CRP) provides/tracks Veterans' supporting information and folders for claims and requests. Veterans Benefits Management System (VBMS) stores Portable Document Format (PDF) images of submitted forms. Veteran Identity/Eligibility Report System (VIERS) provides DoD interoperability with Veteran Resource Management (VRM) applications. Virtual Lifetime Electronic Record Data Access Service (VLER DAS) provides electronic record access. Virtual VA (VVA) is used to scan forms and documents to online folders.

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.

EVSS is located at the AITC and not at any other site.

3. Legal Authority and SORN

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

The legal authority for the Enterprise Veterans Self Service Portal is Title 38 U.S.C. Section 5106 and System of Records Notice (SORN) 58VA21/22/28.System title is Compensation, Pension, Education, and Vocational Rehabilitation and Employment.

The Privacy Act of 1974, set forth at 5 U.S.C. 552a, states the legal authority to utilize this information. As per the SORN, The U.S. government is authorized to ask for this information under Executive Orders 9397, 10450, 10865, 12333, and 12356; sections 3301 and 9101 of title 5, U.S. Code; sections 2165 and 2201 of title 42, U.S. Code; sections 781 to 887 of title 50, U.S. Code; parts 5, 732, and 736 of title 5, Code of Federal Regulations; and Homeland Security Presidential Directive 12.

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?*
No.

D. System Changes

J. *Whether the completion of this PIA will result in circumstances that require changes to business processes*
No.

K. *Whether the completion of this PIA could potentially result in technology changes*
No.

Section 1. Characterization of the Information

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

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

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

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

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

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

☒ Name
☒ Social Security Number
☒ Date of Birth
☐ Mother's Maiden Name
☒ Personal Mailing Address
☒ Personal Phone Number(s)
☐ Personal Fax Number
☒ Personal Email Address
☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☒ Financial Information

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

☐ Integrated Control Number (ICN)
☐ Military History/Service Connection
☐ Next of Kin
☐ Other Data Elements (list below)

PII Mapping of Components (Servers/Database)

Enterprise Veterans Self Service Portal consists of 0 key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by EVSS 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
N/A	N/A	N/A	N/A	N/A	N/A

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?

EVSS receives the information directly from veterans as they input their data into the EVSS application.

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.

EVSS interfaces with other systems to present veterans with their VA benefits, data and profile.

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

EVSS does not create or change 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?

EVSS receives the information directly from veterans as they input their data into the EVSS application. EVSS interfaces with other systems to present veterans with their VA benefits, data and profile.

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.

Forms completed electronically within EVSS are Dependent Claim (VA Form 21-686c/VA Form 21-674) OMB Approved No. 2900-0043/2900-0049, Compensation Claim (VA Form 526ez/VA Form 4502) OMB Approval No. 2900-0747/2900-0067, Request for Representation (21-22/A) OMB Control No. 2900-0321, Request for Release of Medical Information (VA Form 21-4142/A) OMB Control No. 2900-0001, Claim for PTSD (VA Form 781/A) OMB Control No.2900-659 and Claim for Condition of Unemployability (VA Form 21-8940) OMB Approval No.2900-0404.

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.

Veteran input is manual, and accuracy is dependent on submitter. Data received from another electronic system is checked or verified before ingesting resulting in an error notice/alert.

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.

Authentication information as submitted by Veteran/service member/family member is verified against connection authentication information before any information is passed to EVSS.

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

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

The legal authority for Enterprise Veterans Self Service Portal is Title 38, United States Code, Section 5106. The head of any Federal department or agency shall provide such information to the Secretary as the Secretary may request for purposes of determining eligibility for or amount of benefits or verifying other information with respect thereto. The cost of providing information to the Secretary under this section shall be borne by the department or agency providing the information." It is also covered by SORN 58VA21/22/28. System title is Compensation, Pension, Education, and Vocational Rehabilitation and Employment. https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

The Privacy Act of 1974, set forth at 5 U.S.C. 552a, states the legal authority to utilize this information. As per the SORN, The U.S. government is authorized to ask for this information under Executive Orders 9397, 10450, 10865, 12333, and 12356; sections 3301 and 9101 of title 5, U.S. Code; sections 2165 and 2201 of title 42, U.S. Code; sections 781 to 887 of title 50, U.S. Code; parts 5, 732, and 736 of title 5, Code of Federal Regulations; and Homeland Security Presidential Directive 12.

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: If data is received incorrectly by the veteran there is a risk that the system might not capture the error.

Mitigation: Data received from another electronic system is checked or verified before ingesting resulting in an error notice/alert

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.

EVSS supports the mission by providing access to available benefits from the VA and the Department of Defense and access to a variety of self-service tools, and catalog of links for military and VA benefits, etc. for Veterans, Wounded Warriors, Service Members as well as eligible spouses and dependents.

EVSS allows users to receive personalized and customized information relevant to them, conduct online transactions related to the application for VBA benefits and services, and to maintain those VBA benefits and services.

EVSS supports the mission by providing a single-entry point for web-based access to VA systems and self-service functions by stakeholders, business partners and service providers to streamline the claims, claims support, benefits, benefits support and status of benefits or claims submitted.

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.

EVSS does not analyze, accumulate, or interpret the data they receive or collect; they merely regurgitate it to the appropriate connected applications and/or forms.

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.

EVSS does not analyze, accumulate, or interpret the data they receive or collect; they merely regurgitate it to the appropriate connected applications and/or forms.

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?

IAW FIPS 140-2, EVSS operates to prevent the unauthorized disclosure of the contents of data in transit from the web portal to its VA partners using encryption. EVSS utilized the following data in transit encryption protocols: Simple Object Access Protocol (SOAP) over Hyper Text Transport Secure (HTTPS) and Transport Layer Security (TLS). Data at rest is automatically encrypted and stored in the EVSS databases.

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

IAW FIPS 140-2, EVSS operates to prevent the unauthorized disclosure of the contents of data in transit from the web portal to its VA partners using encryption. EVSS utilized the following data in transit encryption protocols: Simple Object Access Protocol (SOAP) over Hyper Text Transport Secure (HTTPS) and Transport Layer Security (TLS). Data at rest is automatically encrypted and stored in the EVSS databases.

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

IAW FIPS 140-2, EVSS operates to prevent the unauthorized disclosure of the contents of data in transit from the web portal to its VA partners using encryption. EVSS utilized the following

data in transit encryption protocols: Simple Object Access Protocol (SOAP) over Hyper Text Transport Secure (HTTPS) and Transport Layer Security (TLS). Data at rest is automatically encrypted and stored in the EVSS databases.

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?

Veteran's PII is only accessible by the Veteran who owns it. Veterans access the EVSS portal, click on login and they have three ways- DS logon account, ID.me account and login.gov. They can see their user profiles and see all the data they entered. Access for VA employees and contractors are requested by supervisors and/COR's through ePASS which is then approved by the COR and ISO.

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

Yes. EVSS Access Request Standard Operating Procedures (SOP).

2.4c Does access require manager approval?

For VA employees and contractors, manager approval is required to access EVSS.

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

Yes. The Database monitors, tracks, and records PII.

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

The EVSS team is responsible for safeguarding PII by using FIPSS 140-2 encryption for PII in transit.

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*

No PII and PHI is retained by EVSS; it is passed to/received from the data source partners.

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.*

No PII or PHI is retained by EVSS, data is received from the veteran into the EVSS web portal and then passed on to the data source systems.

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

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

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

No PII or PHI is retained by EVSS, data is received from the veteran into the EVSS web portal and then passed on to the data source systems.

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

No PII or PHI is retained by EVSS, data is received from the veteran into the EVSS web portal and then passed on to the data source systems.

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.

No PII or PHI is retained by EVSS, data is received from the veteran into the EVSS web portal and then passed on to the data source systems.

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.

No PII or PHI is retained by EVSS, data is received from the veteran into the EVSS web portal and then passed on to the data source systems

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: EVSS receives data but cannot push the data to the receiving systems.

Mitigation: EVSS stores veterans' data in a secured queue while awaiting an automatic transmission to the system of record.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Benefits Gateway Services (BGS)	Eligibility and Entitlement	Veteran SSN/File, Number/Service/Number/Insurance Number, Spouse / Children (Dependent) SSN, Veteran / Spouse / Children (Dependent) Name, Veteran Address, Veteran Email, Veteran Phone Number, Veteran Health Information, Marital Status, Veteran / Spouse / Children (Dependent) DOB, Veteran Financial Institution Information, Veteran Claim Status / Number, Veteran Disability Claims / PTSD Diagnosis, VSO Name and VSO organization.	Simple Object Access Protocol (SOAP) over Hyper Text Transport Protocol Secure (HTTPS)
Benefits Delivery Network (BDN)	Eligibility and Entitlement	Veteran SSN/File, Number/Service/Number/Insurance Number, Spouse / Children (Dependent) SSN, Veteran / Spouse / Children (Dependent) Name, Veteran Address, Veteran Email, Veteran Phone Number, Veteran Health Information, Marital Status, Veteran / Spouse / Children (Dependent) DOB, Veteran Financial Institution Information, Veteran Claim Status / Number, Veteran Disability Claims / PTSD Diagnosis, VSO Name and VSO organization.	HTTPS
Compensation and Pension (C&P)	Eligibility and Entitlement	Veteran SSN/File, Number/Service/Number/Insurance Number, Spouse / Children (Dependent) SSN, Veteran / Spouse / Children (Dependent) Name, Veteran Address, Veteran Email, Veteran Phone Number, Veteran Health Information, Marital Status, Veteran / Spouse / Children (Dependent) DOB, Veteran	HTTPS

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		Financial Institution Information, Veteran Claim Status / Number, Veteran Disability Claims / PTSD Diagnosis, VSO Name and VSO organization.	
Beneficiary Identification Records Locator Subsystem (BIRLS)	Eligibility and Entitlement	Veteran SSN/File, Number/Service/Number/Insurance Number, Spouse / Children (Dependent) SSN, Veteran / Spouse / Children (Dependent) Name, Veteran Address, Veteran Email, Veteran Phone Number, Veteran Health Information, Marital Status, Veteran / Spouse / Children (Dependent) DOB, Veteran Financial Institution Information, Veteran Claim Status / Number, Veteran Disability Claims / PTSD Diagnosis, VSO Name and VSO organization.	HTTPS
Chapter 33 (CH33)	Eligibility and Entitlement	Veteran SSN/File, Number/Service/Number/Insurance Number, Spouse / Children (Dependent) SSN, Veteran / Spouse / Children (Dependent) Name, Veteran Address, Veteran Email, Veteran Phone Number, Veteran Health Information, Marital Status, Veteran / Spouse / Children (Dependent) DOB, Veteran Financial Institution Information, Veteran Claim Status / Number, Veteran Disability Claims / PTSD Diagnosis.	SOAP over HTTPS
Compensation & Pension Corporate Applications (CRP)	Eligibility and Entitlement	Veteran SSN/File, Number/Service/Number/Insurance Number, Spouse / Children (Dependent) SSN, Veteran / Spouse / Children (Dependent) Name, Veteran Address, Veteran Email,	HTTPS

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		Veteran Phone Number, Veteran Health Information, Marital Status, Veteran / Spouse / Children (Dependent) DOB, Veteran Financial Institution Information, Veteran Claim Status / Number, Veteran Disability Claims / PTSD Diagnosis.	
Federal Case Management Tool (FCMT)	Eligibility and Entitlement	Veteran SSN/File, Number/Service/Number/Insurance Number, Spouse / Children (Dependent) SSN, Veteran / Spouse / Children (Dependent) Name, Veteran Address, Veteran Email, Veteran Phone Number, Veteran Health Information, Marital Status, Veteran / Spouse / Children (Dependent) DOB, Veteran Financial Institution Information, Veteran Claim Status / Number, Veteran Disability Claims / PTSD Diagnosis, VSO Name and VSO organization.	SOAP over HTTPS
Identity Access Management	Eligibility and Entitlement	Veteran SSN/File, Number/Service/Number/Insurance Number, Spouse / Children (Dependent) SSN, Veteran / Spouse / Children (Dependent) Name, Veteran Address, Veteran Email, Veteran Phone Number, Veteran Health Information, Marital Status, Veteran / Spouse / Children (Dependent) DOB, Veteran Financial Institution Information, Veteran Claim Status / Number, Veteran Disability Claims / PTSD Diagnosis, VSO Name and VSO organization.	HTTPS/SAML

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
Loan Guaranty Service (LGY)	Eligibility and Entitlement	Veteran SSN/File, Number/Service/Number/Insurance Number, Spouse / Children (Dependent) SSN, Veteran / Spouse / Children (Dependent) Name, Veteran Address, Veteran Email, Veteran Phone Number, Veteran Health Information, Marital Status, Veteran / Spouse / Children (Dependent) DOB, Veteran Financial Institution Information, Veteran Claim Status / Number, Veteran Disability Claims / PTSD Diagnosis VSO Name and VSO organization.	HTTPS
Master Veteran Index/Person Services Identity Management (MVI/PSM)	Eligibility and Entitlement	Veteran SSN/File, Number/Service/Number/Insurance Number, Spouse / Children (Dependent) SSN, Veteran / Spouse / Children (Dependent) Name, Veteran Address, Veteran Email, Veteran Phone Number, Veteran Health Information, Marital Status, Veteran / Spouse / Children (Dependent) DOB, Veteran Financial Institution Information, Veteran Claim Status / Number, Veteran Disability Claims / PTSD Diagnosis VSO Name and VSO organization.	HTTPS/SAML
My HealtheVet (MHV)	Eligibility and Entitlement	Veteran SSN/File, Number/Service/Number/Insurance Number, Spouse / Children (Dependent) SSN, Veteran / Spouse / Children (Dependent) Name, Veteran Address, Veteran Email, Veteran Phone Number, Veteran Health Information, Marital Status, Veteran / Spouse / Children (Dependent) DOB, Veteran	SOAP over HTTPS

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		Financial Institution Information, Veteran Claim Status / Number, Veteran Disability Claims / PTSD Diagnosis VSO Name and VSO organization.	
Office of General Council (OGC)	Eligibility and Entitlement	Veteran SSN/File, Number/Service/Number/Insurance Number, Spouse / Children (Dependent) SSN, Veteran / Spouse / Children (Dependent) Name, Veteran Address, Veteran Email, Veteran Phone Number, Veteran Health Information, Marital Status, Veteran / Spouse / Children (Dependent) DOB, Veteran Financial Institution Information, Veteran Claim Status / Number, Veteran Disability Claims / PTSD Diagnosis, VSO Name and VSO organization.	SOAP over HTTPS
The Image Management Systems (TIMS)	Eligibility and Entitlement	Veteran SSN/File, Number/Service/Number/Insurance Number, Spouse / Children (Dependent) SSN, Veteran / Spouse / Children (Dependent) Name, Veteran Address, Veteran Email, Veteran Phone Number, Veteran Health Information, Marital Status, Veteran / Spouse / Children (Dependent) DOB, Veteran Financial Institution Information, Veteran Claim Status / Number, Veteran Disability Claims / PTSD Diagnosis, VSO Name and VSO organization.	HTTPS
VA Corporate Web Environment (WBT) Benefits Enterprise Platform (BEP)	Eligibility and Entitlement	Veteran SSN/File, Number/Service/Number/Insurance Number, Spouse / Children (Dependent) SSN, Veteran / Spouse / Children (Dependent) Name, Veteran Address, Veteran Email,	HTTPS

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		Veteran Phone Number, Veteran Health Information, Marital Status, Veteran / Spouse / Children (Dependent) DOB, Veteran Financial Institution Information, Veteran Claim Status / Number, Veteran Disability Claims / PTSD Diagnosis, VSO Name and VSO organization.	
VA DoD Identity Repository (VADIR)	Eligibility and Entitlement	Veteran SSN/File, Number/Service/Number/Insurance Number, Spouse / Children (Dependent) SSN, Veteran / Spouse / Children (Dependent) Name, Veteran Address, Veteran Email, Veteran Phone Number, Veteran Health Information, Marital Status, Veteran / Spouse / Children (Dependent) DOB, Veteran Financial Institution Information, Veteran Claim Status / Number, Veteran Disability Claims / PTSD Diagnosis, VSO Name and VSO organization.	HTTPS/SAML
Veterans Appeals Control and Location System (VACOLS)	Eligibility and Entitlement	Veteran SSN/File, Number/Service/Number/Insurance Number, Spouse / Children (Dependent) SSN, Veteran / Spouse / Children (Dependent) Name, Veteran Address, Veteran Email, Veteran Phone Number, Veteran Health Information, Marital Status, Veteran / Spouse / Children (Dependent) DOB, Veteran Financial Institution Information, Veteran Claim Status / Number, Veteran Disability Claims / PTSD Diagnosis, VSO Name and VSO organization.	JDBC protected by TLS
Veterans Authorizations and	Eligibility and Entitlement	Veteran SSN/File, Number/Service/Number/Insurance	HTTPS/WRSP

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
Preferences (NVP/VAP)		Number, Spouse / Children (Dependent) SSN, Veteran / Spouse / Children (Dependent) Name, Veteran Address, Veteran Email, Veteran Phone Number, Veteran Health Information, Marital Status, Veteran / Spouse / Children (Dependent) DOB, Veteran Financial Institution Information, Veteran Claim Status / Number, Veteran Disability Claims / PTSD Diagnosis, VSO Name and VSO organization.	
Veterans Benefit Management System (VBMS)	Eligibility and Entitlement	Veteran SSN/File, Number/Service/Number/Insurance Number, Spouse / Children (Dependent) SSN, Veteran / Spouse / Children (Dependent) Name, Veteran Address, Veteran Email, Veteran Phone Number, Veteran Health Information, Marital Status, Veteran / Spouse / Children (Dependent) DOB, Veteran Financial Institution Information, Veteran Claim Status / Number, Veteran Disability Claims / PTSD Diagnosis, VSO Name and VSO organization.	SOAP over HTTPS
Veteran Identity/Eligibility Report System (VIERS)	Eligibility and Entitlement	Veteran SSN/File, Number/Service/Number/Insurance Number, Spouse / Children (Dependent) SSN, Veteran / Spouse / Children (Dependent) Name, Veteran Address, Veteran Email, Veteran Phone Number, Veteran Health Information, Marital Status, Veteran / Spouse / Children (Dependent) DOB, Veteran Financial Institution Information, Veteran Claim Status	Enterprise Java Bean (EJB) protected by Transport Layer Security (TLS)

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		/ Number, Veteran Disability Claims / PTSD Diagnosis, VSO Name and VSO organization.	
Virtual Lifetime Electronic Record Data Access Service (VLER DAS)	Eligibility and Entitlement	Veteran SSN/File, Number/Service/Number/Insurance Number, Spouse / Children (Dependent) SSN, Veteran / Spouse / Children (Dependent) Name, Veteran Address, Veteran Email, Veteran Phone Number, Veteran Health Information, Marital Status, Veteran / Spouse / Children (Dependent) DOB, Veteran Financial Institution Information, Veteran Claim Status / Number, Veteran Disability Claims / PTSD Diagnosis, VSO Name and VSO organization.	HTTPS/WRSP
Veteran Service Network (VET) Share	Eligibility and Entitlement	Veteran SSN/File, Number/Service/Number/Insurance Number, Spouse / Children (Dependent) SSN, Veteran / Spouse / Children (Dependent) Name, Veteran Address, Veteran Email, Veteran Phone Number, Veteran Health Information, Marital Status, Veteran / Spouse / Children (Dependent) DOB, Veteran Financial Institution Information, Veteran Claim Status / Number, Veteran Disability Claims / PTSD Diagnosis, VSO Name and VSO organization.	SOAP over HTTPS
Virtual VA (VVA)	Eligibility and Entitlement	Veteran SSN/File, Number/Service/Number/Insurance Number, Spouse / Children (Dependent) SSN, Veteran / Spouse / Children (Dependent) Name, Veteran Address, Veteran Email, Veteran Phone Number,	HTTPS

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		Veteran Health Information, Marital Status, Veteran / Spouse / Children (Dependent) DOB, Veteran Financial Institution Information, Veteran Claim Status / Number, Veteran Disability Claims / PTSD Diagnosis, VSO Name and VSO organization.	

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: The sharing of data is necessary for the support of claims and benefits for eligible Veterans at Stakeholder Enterprise Portal. However, there is a risk that the data could be shared with an inappropriate VA organization which would have a potentially catastrophic impact on privacy.

Mitigation: Consent for use of PII data is signaled by completion and submission of claims/benefits forms by the Veteran. The principle of need to know is strictly adhered to. Only personnel with a clear business purpose are allowed access to the system and information contained within. Review of access to all systems is done on a quarterly basis by the ISO and the security engineer. Clearance is required for each person accessing the system.

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

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: An external parties could hack into the system.

Mitigation: VA employs security in depth, systems hardening, annual security and privacy awareness training for VA employees.

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 EVSS information system relies an approved, standardized notification message and consent to monitoring message to potential users prior to granting system access on the DoD DS-Logon side. It does maintain a privacy acceptance field within its transaction history that each user must complete within that user's temporary profile that acknowledges privacy information will be transmitted or displayed with the Veteran's (user's) consent. This Privacy Impact Assessment (PIA) serves as a public notice that the EVSS exists and displays/transmits and individual's information. SORN 58VA21/22/28. System title is Compensation, Pension, Education, and Vocational Rehabilitation and Employment. All privacy related topics are found here. VA Privacy Service

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

https://www.ebenefits.va.gov/ebenefits/homepage.

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

This Privacy Impact Assessment (PIA) serves as a public notice that the EVSS exists and displays/transmits individual's information. SORN 58VA21/22/28. System title is Compensation, Pension, Education, and Vocational Rehabilitation and Employment

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.

Failure to provide information results in limitation of what the user can access in the information system. Benefits application information is required for the VA to provide benefits to any given veteran. While there is no penalty for not supplying information, a lack of information will limit the type of benefits that the VA can provide.

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.

There is no process other than the privacy acceptance question within the EVSS transaction history to limit privacy consent. Veterans may have the opportunity or notice of right to decline to provide information to the source data partners noted in Section 1.1 that collect the information from the Veteran.

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:

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

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

Privacy Risk: There is a risk that an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by the EVSS.

Mitigation: The VA mitigates this risk by publishing this Privacy Impact Assessment on a public website. https://www.oprm.va.gov/privacy/pia.aspx

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.***

Veteran access is dependent on pre-screening through Defense Enrollment Eligibility Reporting System (DEERS) and acquiring a Department of Defense Self-Service Logon (DS Logon) account, DS Logon - DMDC (osd.mil). Vets.gov access is conducted prior to connection to EVSS. All Veterans who are receiving VA Benefits are mailed a Health Benefits handbook. The handbook includes such things as their benefits, factors that went into their enrollment decision, contact information for their medical facility and instructions for what to do if their information is incorrect. Veterans can update their records or follow guidance from the system of records notice SORN 58VA21/22/28. System title is Compensation, Pension, Education, and Vocational Rehabilitation and Employment.

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).

EVSS is not exempt from 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.

EVSS is a Privacy Act system.

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

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

Veterans can request an amendment of records by following guidance from the system of records notice SORN 58VA21/22/28. System title is Compensation, Pension, Education, and Vocational Rehabilitation and Employment.

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.

Veterans and authorized parties have a statutory right to request a copy of or an amendment to a record in VA's possession at any time under the Freedom of Information Act (FOIA) and the Privacy Act (PA). VA has a decentralized system for fulfilling FOIA and PA requests. The type of information or records an individual is seeking will determine the location to which a request should be submitted. For records contained within a VA claims folder (Compensation and Pension claims), or military service medical records in VA's possession, the request will be fulfilled by the VA Records Management Center. Authorized requestors should mail their Privacy Act or FOIA requests to: Department of Veterans Affairs, Claims Intake Center, P.O. Box 4444, Janesville, WI 53547–4444, DID: 608–373–6690. For other benefits records maintained by VA (to include Vocational Rehabilitation & Employment, Insurance, Loan Guaranty or Education Service) submit requests to the FOIA/ Privacy Act Officer at the VA Regional Office serving the individual's jurisdiction. Address locations for the nearest VA Regional Office are listed at VA Locations Link. Any individuals who have questions about access to records may also call 1– 800–327–1000. Information about how to contact Fiduciary services can be found here: https://www.benefits.va.gov/FIDUCIARY/contact-us.asp.

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.

Veterans would log in to the eBenefits portal and update their records.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

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

Mitigation: The information displayed in EVSS is obtained from many other systems. If there is erroneous or inaccurate information, it needs to be addressed in those systems. Any validation performed would merely be the Veteran personally reviewing the information before they provide it. Individuals are allowed to provide updated information for their records by submitting new forms or correspondence and indicating to the VA that the new information supersedes the previous data. There is a contact desk button with a HELP section.

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.

Veteran uses pre-authenticated Logon ID – DS Logon. For more information regarding what a DoD Self-Service Logon is and how to obtain one, refer to the DoD's http://www.va.gov/EAUTH/DSLogon.asp.PII, PHI and SPI is not shared with any of the system administrators.

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

No employees from other government agencies do not have access to EVSS.

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.

Personnel who will be accessing information systems must read and acknowledge their receipt and acceptance of the VA Information Security Rules of Behavior (RoB) prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training that all personnel must complete via the VA's 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 obtained through electronic acknowledgment is tracked through the TMS system. All VA employees must complete annual Privacy and Security training. This training includes, but is not limited to, the following TMS Courses:
. VA 10176: Privacy and Info Security Awareness and Rules of Behavior
. VA 10203: Privacy and HIPAA Training
. VA 3812493: Annual Government Ethics Role-based Training

Includes, but is not limited to and based on the role of the user.
VA 1016925: Information Assurance for Software Developers IT Software Developers
VA 3195: Information Security for CIOs Executives, Senior Managers, CIOs and CFOs
VA 1357084: Information Security Role-Based Training for Data Managers
VA 64899: Information Security Role-Based Training for IT Project Managers
VA 3197: Information Security Role-Based Training for IT Specialists
VA 1357083: Information Security Role-Based Training for Network Administrators
VA 1357076: Information Security Role-Based Training for System Administrators
VA 1337064: Information Security for Facilities Engineers

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.

Yes, VA contractors' access the EVSS system. The majority of the development team is comprised of contractors who sign Non-Disclosure Agreements. The System Administrator team is also comprised of contractors. Access to the systems for both teams is required for ongoing software development work to continue as well as for day-to-day maintenance of the systems and their networks. Review of access to all systems is done on a quarterly basis by the Information System Owner (ISO) and the security engineer. Clearance is required for each person accessing the system.

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 (for AITC technicians) prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the Rules, the user must 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. All VA employees must complete annual Privacy and Security training. Users agree to comply with all terms and conditions of the National Rules of Behavior, by signing a certificate of training at the end of the training session. All VA and contractor employees who work on EVSS must take a Privacy Training and Privacy Rules of Behavior.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* SSP is in place and approved
2. *The System Security Plan Status Date:* 10-31-2022
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* 09-Jan-2023
5. *The Authorization Termination Date:* 13-Apr-2023
6. *The Risk Review Completion Date:* 07-Dec-2022
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* 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 (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)*

EVSS does not use cloud technology.

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

EVSS does not use cloud technology.

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

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

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

EVSS does not use cloud technology.

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

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

EVSS does not use cloud technology.

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

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

EVSS does not use any RPA.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

ID	Privacy Controls
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.

JEAN-CLAUDE WICKS

Digitally signed by JEAN-CLAUDE WICKS
Date: 2023.04.10 09:51:43 -06'00'

Privacy Officer, Jean-Claude Wicks

JOSEPH FACCIOLLI

Digitally signed by JOSEPH FACCIOLLI
Date: 2023.04.10 08:04:46 -04'00'

Information Systems Security Officer, Joseph Facciolli

Dale K. Beehler 519351

Digitally signed by Dale K. Beehler 519351
Date: 2023.04.07 15:19:42 -04'00'

Information System Owner, Dale Beehler

APPENDIX A-6.1

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

https://www.ebenefits.va.gov/ebenefits/homepage

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