Privacy Impact Assessment for the VA IT System called:

Benefits Enterprise Platform (BEP)

Veteran Benefits Administration (VBA)

Office of Business Integration (OBI)

Date PIA submitted for review:

07/19/2023

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)	Tamer Ahmed	Tamer.Ahmed@va.gov	202-461-9306
Information System Owner	Derolyn Dozier	Derolyn.Dozier@va.gov	630-414-3253

Abstract

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

The Benefits Enterprise Platform (BEP) is an Enterprise Architecture (EA) General Support System (GSS) that provides service delivery via web-based technologies (WBT) and service-oriented architectures (SOA) for a variety of Veterans Benefits Administration (VBA) business systems.

BEP servers execute Common Security Services (CSS), Veteran Service Network (VETSNET) applications, and the applications and batch files that make up the Personal Information Exchange System (PIES) to client workstations at 57 VBA Regional Offices as well in the VBA Citrix environment.

The overall purpose of BEP is to provide information flow between the VBA Corporate Database (CRP) and VBA client systems which consume, update and process CRP records in support of their individualized business process needs. VBA client business systems include, but are not limited to, Compensation and Pension, Education, Vocational Rehab and Employment, Insurance, Loan Guaranty etc.

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.

- The Benefits Enterprise Platform (BEP) is owned by the VBA Office of Business Integration (OBI) and operated by Benefits Integration and Administration (BIA) Product Line which is situated within the Benefits and Memorials (BAM) Portfolio.

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

- The overall purpose of BEP is to provide information flow between VBA Corporate Database (CRP) and VBA client systems which consume, update and process CRP records in support of their individualized business process needs. VBA client business systems include, but are not limited to, Compensation and Pension, Education, Vocational Rehab and Employment, Insurance, Loan Guaranty etc.

- BEP servers execute CSS, VETSNET applications, and the applications and batch files that make up the PIES to client workstations at 57 VBA Regional Offices as well in the VBA Citrix environment.

- CSS is the underlying security application providing access and authentication services to in-house developed VBA client-server and Web-Logic applications. CSS controls who, and to what extent, VA employees and Veteran Service Officers (VSOs), can access data within CRP for the purpose of accessing, establishing, and developing Veterans' claims.

- VETSNET is a suite of applications that facilitates the Compensation and Pension (C&P) claims process. Within the suite, the end user can establish and develop Veterans' claims; the rating decision, award and notification letter are documented; and payment information is transmitted to Treasury, accomplishing the necessary accounting. Throughout these activities, data passed between the applications to support end-to-end claims processing, customer service and notification.

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

- The Benefits Enterprise Platform (BEP) is owned by the VBA OBI and operated by the BIA Product Line, which is situated within the BAM Portfolio.

2. Information Collection and Sharing

- BEP collects and processes but does not retain information. BEP provides information flow between the CRP and VBA client systems which consume, update and process CRP records in support of their individualized business process needs. The CRP serves as a central repository and system of record for Veteran and related benefits information.

D. The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual

- BEP collects and processes but does not retain any information. All information is stored within CRP. Information regarding the type of individual and/or expected number of individuals whose information is stored beyond the scope of BEP

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

- BEP collects but does not retain any information. BEP is a mechanism for sharing information between the VBA CRP and internal VA systems for the purpose of processing Veteran Awards, Claims and Ratings. and Claims.

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

- BEP is a mechanism for sharing information between CRP and internal VA systems for the purpose of processing Veteran Awards, Claims and Ratings.

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.

- BEP is physically housed within the Austin and Philadelphia VA Information Technology Centers (ITC). All data is encrypted in transmission and at rest within the database.

3. Legal Authority and SORN

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

- VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records— VA'' (58VA21/22/28)
  - https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf
- Legal authority to maintain the system is: 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

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?*
- N/A

D. System Changes

J. *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- Completion of this PIA is not anticipated to result in circumstances that require changes to business process.

K. *Whether the completion of this PIA could potentially result in technology changes*
- Completion of this PIA is not anticipated to result in technology changes.

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)

Active/Inactive Indicator, AD User ID, Applications Assigned, Benefits Delivery Network (BDN)Employee Identifier Number (EIN), City and State of Birth, Contract/Work Study End Date, BEP-CSS User Identifier, Financial Information (DD/EFT), Date of Death, Email Address (VA), Duty Station, Fax Number, Foreign Service Number, Functions Assigned, GS Level, Job Code. Job Templates, Job Title, Locked Reason, Military Indicator Type, Organization/Division, Pager Number, Payment Address, Personal/Evening Phone Number, Rating Information, Registry Number, Role Assigned, Sensitive Access Level, Service Code. CSS User's Supervisor's Name and Job Title, BEP-CSS User's Supervisor's Phone Number, BEP-CSS User's Supervisor, VA Claim Number, VA File Number. Veteran Service Officer (VSO) Indicator, Work Phone Number, Veteran Type, Various Financial and Claims Information, Organization Code, Military Decoration, Disability/Percent of Disability, Competency, Character of Discharge, Service Dates, Master Earnings File Number, Parents Names

PII Mapping of Components (Servers/Database)

Benefits Enterprise Platform (BEP) consists of **20** key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **BEP** 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
VBA Corporate Database (CRP)	Yes	Yes	First, Middle and Last Name, DOB, SSN, Address, Email Address, Phone Number, Rating Information, Financial information, BDN EIN, VA Claim Number	Eligibility determinations within the claims processing lifecycle.	• All Users, employees and contractors, are required to take VA Privacy and Rules of Behavior, which includes training on how to safeguard PII/PHI.

			and CSS User Identification.		• Users must be authorized via Common Security Services (CSS). • All data is encrypted at rest in the database.
Benefits Delivery Network (BDN)	Yes	Yes	First, Middle and Last Name, DOB, Address, Phone Number, SSN, Rating Information, DD/EFT Information.	Eligibility determinations within the claims processing lifecycle.	• Users, employees and contractors, are required to take VA Privacy and Rules of Behavior, which includes training on how to safeguard PII/PHI. • Users must be authorized via Common Security Services (CSS). • All data is encrypted at rest in the database.

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?

- BEP processes information, listed above in Section 1.1, from the VBA CRP, BDN and partner systems for the purpose of processing Veteran Awards, Claims, Ratings etc.

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.

- BEP processes information, listed above in Section 1.1, from the VBA CRP, BDN and partner systems for the purpose of processing Veteran Awards, Claims, Ratings etc.

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

- N/A

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?

- BEP processes information, listed above in Section 1.1, from the internal VA systems for the purpose of processing Veteran Awards, Ratings and Claims. This information is collected directly from individuals who are the subject of the information through VA source systems however this is beyond the scope BEP.

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.

- N/A

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.

- BEP does not manage the data validation processes and assumes that the original source data has been reviewed for accuracy before being added to the source system. Data may be checked for completeness by system audits, manual verifications, annual questionnaires through automated Veteran letters via VA source systems however that is outside the scope of BEP.

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.

- N/A

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

- VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records— VA'' (58VA21/22/28)
    - https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf
- Legal authority to maintain the system is: 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

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: 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 the information processed by BEP was breached or accidentally released to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to the individuals whose information is processed by the system.

Mitigation: All employees with access to Veteran's information are required to complete the VA Privacy, Information Security Awareness and Rules of Behavior Training annually. All data is encrypted at rest in the database as well as in transmission. SSNs are protected via a least privilege, RBAC (rules-based access control) through the CSS. Data is also protected via the implementation of Sensitivity Levels, whereby users must be granted specific Sensitivity levels from their ISSO to see specific information.

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.

Information Type	Purpose
Active/Inactive Indicator	To determine if the BEP-CSS User is still active
AD User ID	To determine the BEP-CSS User's access rights and permission levels
Applications Assigned	To determine the BEP-CSS User will be accessing
Benefits Delivery Network (BDN)Employee Identifier Number (EIN)	To determine the BEP-CSS User's access rights and permission levels
City and State of Birth	To identify the Veteran and/or claimant
Contract/Work Study End Date	To indicate the BEP-CSS User's contract/work study end date to ensure the User's record will be automatically locked (in case the contract is not renewed). If the contract is renewed, the ISO or Security Officer will update the Contract End Date so the User can resume their access.
BEP-CSS User Identifier	To determine if the BEP-CSS User's access rights and permission levels
Date of Birth	To identify the Veteran and/or claimant
Financial Information (DD/EFT)	To provide payment to the Veteran or claimant
Date of Death	To identify the day of passing for Veteran
Emergency Contact	To obtain emergency contact information
Email Address (VA)	To match the BEP-CSS Users Active Directory User ID with the BEP-CSS User ID using the employee's e-mail address
Email Address (personal)	To correspond with the Veteran and/or claimant as well as confirm the Veterans identity
Duty Station	To identify what station the BEP-CSS User will login to when accessing VBA Applications
Fax Number	To contact the BEP-CSS User, Veteran and/or claimant
Foreign Service Number	To identify the exact Veteran or claimant based on Foreign Service
Functions Assigned	To determine the BEP-CSS User's access rights and permission levels
Gender	To identify Veteran and/or claimant
GS Level	To ensure BEP-CSS Users are only allowed to perform functions that are appropriate to their GS level
Job Code	To identifies the office of the BEP-CSS User, but is not stored in CSS and is mainly used by HR

Job Templates	To expedite access requests for BEP-CSS Users
Job Title	To determine the type of work the BEP-CSS User will be doing within the VBA System
Locked Reason	To determine why a BEP-CSS User's account is locked
Mailing Address	To correspond with the Veteran and/or claimant
Military Indicator Type	To identify what vertical/branch Veteran belongs
Mother's Maiden Name	To confirm the Veterans identity
Name (First, Last, MI)	To identify BEP-CSS User, Veteran and/or claimant
Organization/Division Code	To gain access to supervisor information so that CSEM Electronic access requests may be approved properly by the BEP-CSS User's supervisor
Pager Number	To contact the CSS User, Veteran and/or claimant
Payment Address	To provide payment to the Veteran and/or claimant
Personal/Evening Phone Number	To contact the CSS User, Veteran and/or claimant
Rating Information	To identify the information related to disabilities reported by the Veteran and the disability rating assigned to it based on the severity of the disability
Registry Number	To provide additional information regarding a CSS User's Foreign Service Number
Role Assigned	To determine the BEP-CSS User's access rights and permission levels
Sensitive Access Level	To specify the record level the BEP-CSS User is allowed to access within the sensitive file for those Veterans who have their record sensitized
Service Code	To determine a transactions point of origin
SSN	To process Veteran and/or claimant claim payments per IRS and SSN requirements.
BEP-CSS User's Supervisor's Name and Job Title	To verify the BEP-CSS User's Supervisor
BEP-CSS User's Supervisor's Phone Number	To verify the BEP-CSS User's Supervisor
BEP-CSS User's Supervisor	Supervisor is required to place the employee in the correct division so the supervisor can approve all electronic requests for access through CSEM
VA Claim Number	To identify the Veteran and/or claimant.
VA File Number	Only collected if the employee or external entity is a Veteran
Veteran Service Officer (VSO) Indicator	To determine whether the BEP-CSS User is a VSO
Work Phone Number	To contact the BEP-CSS User, Veteran and/or claimant
Veteran Type	To identify the Veteran
Various Financial and Claims Information	To process Veteran claims
Military Decoration	To process Veteran claims

Disability/Percent of Disability	To identify the information related to disabilities reported by the Veteran and the disability rating assigned to it based on the severity of the disability
Competency	To process Veteran claims
Character of Discharge	To process Veteran claims
Service Dates	To identify the Veteran
Master Earnings File Number	To process Veteran claims
Parents Names	To identify the Veteran and/or claimant

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.

- BEP does not accumulate, analyze, or interpret the data received or provided.

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.

- BEP does not create or make available new or previously unutilized information about an individual.

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?

- While in transit, the systems utilize Mutual SSL authentication and encryption protocols. All data is encrypted at rest in the database.

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

- All data is encrypted at rest in the database. SSNs are protected via a least privilege, RBAC (rules-based access control) through the CSS. Data is also protected via the implementation of

Sensitivity Levels, whereby users must be granted specific Sensitivity levels from their ISSO to see specific information.

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

- All Users, employees and contractors, are required to take VA Privacy and Rules of Behavior, which includes training on how to safeguard PII/PHI.

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?

- Access to sensitive data is determined via RBAC (rules-based access control) through the CSS.

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

- Yes

2.4c Does access require manager approval?

- Yes

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

- Yes

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

- VA Regional Benefit Office (RBO) ISSO and PO's that are responsible for processing User BEP-CSS access requests.

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

- BEP collects and processes but does not retain any information. All information is stored within CRP, which is beyond the scope of BEP.

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.*

- BEP collects and processes but does not retain any information. All information is stored within CRP, which is beyond the scope of BEP.

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?

- BEP collects and processes but does not retain any information. All information is stored within CRP, which is beyond the scope of BEP.

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

- BEP collects and processes but does not retain any information. All information is stored within CRP, which is beyond the scope of BEP.

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.

- BEP collects and processes but does not retain any information. All information is stored within CRP, which is beyond the scope of BEP.

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.

- All research, testing and/or training is conducted in the lower environments that do not contain PII.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that the information contained in the system will be retained for longer than is necessary to fulfill the VA mission; however, this risk would fall upon the accreditation boundary of the CRP since the PII is maintained within it, not BEP itself.

Mitigation: Mitigation of this risk is the responsibility of CRP.

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 Integration Platform (BIP)	To process veteran claims.	First, Middle and Last Name, DOB, Address, Phone Number, SSN, Rating Information, DD/EFT Information.	HTTPS using Secure Socket Layer encryption certificate.
Salesforce - Caregiver Records Management Application (CARMA)	To process veteran claims	First, Middle and Last Name, DOB, Address, Phone Number, SSN, Rating Information, DD/EFT Information.	HTTPS using Secure Socket Layer encryption certificate.

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*
Caseflow	To process veteran claims	First, Middle and Last Name, DOB, Address, Phone Number, SSN, Rating Information, DD/EFT Information.	HTTPS using Secure Socket Layer encryption certificate.
Vocational Rehabilitation & Employment	To process veteran claims	First, Middle and Last Name, DOB, Address, Phone Number, SSN, Rating Information, DD/EFT Information.	HTTPS using Secure Socket Layer encryption certificate.
Digital GI Bill	To process veteran claims	First, Middle and Last Name, DOB, Address, Phone Number, SSN, Rating Information, DD/EFT Information.	HTTPS using Secure Socket Layer encryption certificate.
BAM CRM Moderate	To process veteran claims	First, Middle and Last Name, DOB, Address, Phone Number, SSN, Rating Information, DD/EFT Information.	HTTPS using Secure Socket Layer encryption certificate.
Enterprise Management of Payments, Workload, and Reporting (eMPWR-VA)	To process veteran claims	First, Middle and Last Name, DOB, Address, Phone Number, SSN, Rating Information, DD/EFT Information.	HTTPS using Secure Socket Layer encryption certificate.
Vocational Rehabilitation and Electronic Virtual Assistant (e-VA)	To process veteran claims	First, Middle and Last Name, DOB, Address, Phone Number, SSN, Rating Information, DD/EFT Information.	HTTPS using Secure Socket Layer encryption certificate.
Enterprise Veterans Self Service Portal (EVSS)	To process veteran claims	First, Middle and Last Name, DOB, Address, Phone Number, SSN, Rating Information, Direct Deposit/Electronic Funds Transfer (DD/EFT) information	HTTPS via BEP using Secure Socket Layer encryption certificate.

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*
Federal Case Management Tool (FCMT)	To process veteran claims	First, Middle and Last Name, DOB, Address, Phone Number, SSN, Rating Information, DD/EFT Information.	HTTPS using Secure Socket Layer encryption certificate.
Web Enabled Approval Management System	To process veteran claims	First, Middle and Last Name, DOB, Address, Phone Number, SSN, Rating Information, DD/EFT Information.	HTTPS using Secure Socket Layer encryption certificate.
Invoice Payment Processing System (IPPS)	To process veteran claims	First, Middle and Last Name, DOB, Address, Phone Number, SSN, Rating Information, DD/EFT Information.	HTTPS using Secure Socket Layer encryption certificate.
Loan Guaranty	To process veteran claims	First, Middle and Last Name, DOB, Address, Phone Number, SSN, Rating Information, DD/EFT Information.	HTTPS using Secure Socket Layer encryption certificate.
Salesforce - Fiduciary Accounting Submission Tool (FAST)	To process veteran claims	First, Middle and Last Name, DOB, Address, Phone Number, SSN, Rating Information, DD/EFT Information.	HTTPS using Secure Socket Layer encryption certificate.
Education Lan Applications	To process veteran claims	First, Middle and Last Name, DOB, Address, Phone Number, SSN, Rating Information, DD/EFT Information.	HTTPS using Secure Socket Layer encryption certificate.
Lighthouse Delivery Infrastructure (LHDI)	To process veteran claims	First, Middle and Last Name, DOB, Address, Phone Number, SSN, Rating Information, DD/EFT Information.	HTTPS using Secure Socket Layer encryption certificate.
Quality Assurance	To process veteran claims	First, Middle and Last Name, DOB, Address, Phone Number, SSN, Rating Information, DD/EFT Information.	HTTPS using Secure Socket Layer encryption certificate.

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*
Identity and Access Management (IAM)	To process veteran claims	First, Middle and Last Name, DOB, Address, Phone Number, SSN, Rating Information, DD/EFT Information.	HTTPS using Secure Socket Layer encryption certificate.
IO Platform Support Mainframe	To process veteran claims	First, Middle and Last Name, DOB, Address, Phone Number, SSN, Rating Information, DD/EFT Information.	HTTPS using Secure Socket Layer encryption certificate.
VA Profile	To process veteran claims	First, Middle and Last Name, DOB, Address, Phone Number, SSN, Rating Information, DD/EFT Information.	HTTPS using Secure Socket Layer encryption certificate.
VBA Automation Platform (VBAAP)	To process veteran claims	First, Middle and Last Name, DOB, Address, Phone Number, SSN, Rating Information, DD/EFT Information.	HTTPS using Secure Socket Layer encryption certificate.
Veterans Enterprise Management System (VEMS)	To process veteran claims	First, Middle and Last Name, DOB, Address, Phone Number, SSN, Rating Information, DD/EFT Information.	HTTPS using Secure Socket Layer encryption certificate.
Veteran Experience Office, Veteran Identity/Eligibility Reporting System	To process veteran claims	First, Middle and Last Name, DOB, Address, Phone Number, SSN, Rating Information, DD/EFT Information.	HTTPS using Secure Socket Layer encryption certificate.
Veterans Benefits Management System (VBMS) Cloud	To process veteran claims	First, Middle and Last Name, DOB, Address, Phone Number, SSN, Rating Information, DD/EFT Information.	HTTPS using Secure Socket Layer encryption certificate.
Veteran Information Solution (VIS)	To process veteran claims	First, Middle and Last Name, DOB, Address, Phone Number, SSN, Rating Information, DD/EFT Information.	HTTPS using Secure Socket Layer encryption certificate.

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*
Salesforce – Whitehouse VA Hotline	To process veteran claims	First, Middle and Last Name, DOB, Address, Phone Number, SSN, Rating Information, DD/EFT Information.	HTTPS using Secure Socket Layer encryption certificate.

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: Sharing of protected Veteran data is necessary to support VA benefits processing/ensure eligible Veterans receive the VA benefits to which they are entitled however sharing of any information carries with it a risk of unauthorized disclosure.

Mitigation: The risk of improperly disclosing protected Veteran data to an unauthorized internal VA entity and/or VA personnel is mitigated by limiting access only those VA entities and personnel with approved access and clear business purpose/need to know. Additionally, consent for use of PII data is signaled by the completion of benefits forms by the Veteran. The principle of need to know is strictly adhered to. Information is shared in accordance with VA Handbook 6500.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
Veterans Service Organization (VSO)	Veterans request assistance of VSO as their power of attorney regarding a claim. These limited powers of attorney authorize the designated organization or individual to act on behalf of the	Active Directory User ID, Last Name, First Name, Middle Name, Suffix, Duty Station, Job Title, GS Level, Job Code, Organization, Division, Work Phone Number, Nighttime Phone Number, VA Email Address, Cell Phone/Pager, Fax Phone Number, Supervisor, Supervisor's Job Title, Supervisor's Phone Number, BDN Employee ID Number, Sensitive Access Level, Veteran Service Officer	VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records— VA'' (58VA21/22/28) states the legal authority to maintain the system is: Title 10 U.S.C. chapters 106a, 510, 1606 and 1607 and Title 38, U.S.C., section	N/A – Access granted through internal VA Account

	claimant in the preparation, presentation, and prosecution of a claim.	Indicator, Organization Codes, Contractor/Work-study End Date, Applications assigned, Roles Assigned, Functions Assigned, Job Templates, Active/Inactive Indicator, Locked Reason.	501(a) and Chapters 11, 13, 15, 18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51, 53, and 55	
State Approving Agency (SAA) Officials	Veterans request assistance of SSA Officials as their power of attorney regarding a claim. These limited powers of attorney authorize the designated organization or individual to act on behalf of the claimant in the preparation, presentation, and prosecution of a claim.	Active Directory User ID, Last Name, First Name, Middle Name, Suffix, Duty Station, Job Title, GS Level, Job Code, Organization, Division, Work Phone Number, Nighttime Phone Number, VA Email Address, Cell Phone/Pager, Fax Phone Number, Supervisor, Supervisor's Job Title, Supervisor's Phone Number, BDN Employee ID Number, Sensitive Access Level, Veteran Service Officer Indicator, Organization Codes, Contractor/Work-study End Date, Applications assigned, Roles Assigned, Functions Assigned, Job Templates, Active/Inactive Indicator, Locked Reason.	VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records— VA'' (58VA21/22/28) states the legal authority to maintain the system is: 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	N/A – Access granted through internal VA Account
VA – Accredited Attorney or Claims Agents	Veterans request assistance of Accredited Attorney or Claims Agents as their power of attorney	Active Directory User ID, Last Name, First Name, Middle Name, Suffix, Duty Station, Job Title, GS Level, Job Code, Organization, Division, Work Phone Number, Nighttime Phone Number, VA Email Address, Cell Phone/Pager, Fax Phone Number,	VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records— VA'' (58VA21/22/28) states the legal authority to	N/A – Access granted through internal VA Account

	regarding a claim. These limited powers of attorney authorize the designated organization or individual to act on behalf of the claimant in the preparation, presentation, and prosecution of a claim.	Supervisor, Supervisor's Job Title, Supervisor's Phone Number, BDN Employee ID Number, Sensitive Access Level, Veteran Service Officer Indicator, Organization Codes, Contractor/Work-study End Date, Applications assigned, Roles Assigned, Functions Assigned, Job Templates, Active/Inactive Indicator, Locked Reason.	maintain the system is: 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	
National Archives and Records Administration (NARA)	To obtain Veteran specific data in support of processing Veteran claims.	SSN/SN, Name, Service Code, Registry Number	ISA (Interconnection Security Agreement)/MOU (memorandum of understanding)	N/A – This information is sent via secure file transfer via email.
Department of Education National Student Loan Data System (NLDS)	To provide VBA an aggregated file allowing VA to post the aggregated institutional-level information on VA's GI Bill Comparison Tool for the Service members,	SSN, Name, DOB	The Privacy Act of 1974 The EGovernment Act of 2002 OMB Circulars and Memoranda: • OMB Circular A-130, Management of Federal Information Resources • OMB M-017-12, Preparing for and Responding to a Breach of Personally Identifiable	Bi-directional file transfer Two-way data files via a Secure File Transfer Protocol using FIPS 140-2 encryption.

	Veterans, to make informed decisions regarding higher education opportunities.		Information • OMB M-08-05, Implementation of Trusted Internet Connections (TIC) Department of Education Policies and Procedures • OCIO 3-112, Cybersecurity Policy • Department of Education Handbook for Protection of Sensitive but Unclassified Information (OCIO-15 • FSA Incident Response Standard Operating Procedures (SOP)	
Department of the Treasury Bureau of the Fiscal Service (TWAI)- TWAI General Support System	To allow the Fiscal Service to share data and information with VA.	SSN, VA File Number, Payment Address (EFT)	Compensation, Pension, Education and Vocational Rehabilitation and Employment Records- VA (58 VA 21/22/28)	Bi-directional connection. All information transferred is FIPS 140-2 compliant
Internal Revenue Service (IRS) Masterfile – International Business Machines	To provide VA income information for purposes of verifying applicants' eligibility and/or payment amounts to recipients under VA benefits programs	SSN, Name, Address, Disability/Percent of Disability, Veteran Type, Service dates, Competency, Character of Discharge	26 U.S.C. 6103 (1)(7) Privacy Act of 1974, 5 U.S.C. 552a 38 U.S.C. 5317	Two-way data exchange: Data is encrypted and transferred using Connect: Direct Secure Plus File Transfer software through a

				VA Transport Layer Protocol site to site VPN tunnel.
Social Security Administration (SSA) and US Department of Health and Human Services Administration for Children and Families Office of Child Support Enforcement and State Bureau of Prisons	• To verify eligibility for Pension Benefits • To complete and determine the amount of the Pension award To determine eligibility for those confined beneficiaries in receipt of VA compensation, pension, or dependency and indemnity compensation, or the amount of VA benefits, and to reduce overpayments.	SSN, Name, DOB, Master Earnings File, Death Indicator, Parents Names	• 38 United States Code (U.S.C.) §§ 5721-5728, Veteran's Benefits, Information Security • 18 U.S.C. § 641Criminal Code: Public Money, Property or Records • 18 U.S.C. § 1905 Criminal Code: Disclosure of Confidential Information • 42 U.S.C. § 653, Federal Parent Locator Service 42 U.S.C. § 654a, Automated Data Processing	Two-way connection protected through FIPS 140-2 approved encryption algorithms and products when encryption required
Social Security Administration (SSA)	• To verify and correct	SSN, DOB, Master Earnings File. Death indicator	• Compensation, Pension, Education	Two-way connection protected

(SSNECS), • Title II Systems (Title II), • Supplemental Security Income Record Maintenance Systems (SSIRMS) and Earnings Records Maintenance System (ERMS) Death Alert Control and Update System (DACUS)	benefit records ensuring certain benefits will properly terminate when there is a record of death.		and Vocational Rehabilitation and Employment Records System of Record (58VA21/22/28)	through FIPS 140-2 approved encryption algorithms and products when encryption require

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: The VA cannot control what authorized users do with the data they view, after they view it; therefore, it could potentially be shared with entities and individuals without proper permissions to access the data; however, that risk would fall on the application through which the user was accessing that is stored within the CRP, not on BEP. BEP does not retain or maintain PII.

Mitigation: 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. All users are required to adhered to all information security requirements instituted by the VBA. Information is shared in

accordance with VA Handbook 6500. All personnel accessing Veteran's information must first have a successfully adjudicated fingerprint check. This fingerprint check is conducted by the Federal Bureau of Investigation (FBI) Justice Information and criminal history records. Individual users are given access to Veteran's data through the issuance of a user ID and password, and by the use of a Personal Identity Verification (PIV) card. This ensures the identity of the user by requiring two-factor authentication.

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.

- VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records— VA'' (58VA21/22/28)
    - https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

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

- N/A

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 is not applicable to BEP as the systems does not engage directly with the Veteran. All data processed by BEP is provided by partner systems as noted in Section 1.1. Veterans may have the opportunity or notice of the right to decline to provide information to the source systems that collects the information from the Veteran.

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.

- This is not applicable to BEP as the systems does not engage directly with the Veteran. All data processed by BEP is provided by partner systems as noted in Section 1.1. Veterans may have the opportunity or notice of the right to decline to provide information to the source systems that collects the information from the Veteran.

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.

- This is not applicable to BEP as the systems does not engage directly with the Veteran. All data processed by BEP is provided by partner systems as noted in Section 1.1. Veterans may have the opportunity or notice of the right to decline to provide information to the source systems that collects the information from the Veteran.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Privacy Risk: An individual may not receive notice that BEP is processing their information.

Mitigation: The VA mitigates this risk by providing Veterans and other beneficiaries with multiple forms of notice of information collection, retention, and processing. The main forms of notice are discussed in the Privacy Act statement, a System of Record Notice, and the publishing of this Privacy Impact Assessment.

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.***

- Individuals seeking information regarding access to and contesting of VA records may write, call, or visit the nearest VA regional office. See VA SORN Compensation, Pension, Education and Employment Records-VA, SORN 58VA21/22/2886 FR 61858 (November 08, 2021).

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).

- N/A

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.

- N/A

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 seeking information regarding access to and contesting of VA records may write, call, or visit the nearest VA regional office. See VA SORN Compensation, Pension, Education and Employment Records-VA, SORN 58VA21/22/2886 FR 61858 (November 08, 2021).

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

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

This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

- Individuals seeking information regarding access to and contesting of VA records may write, call, or visit the nearest VA regional office. See VA SORN Compensation, Pension, Education and Employment Records-VA, SORN 58VA21/22/2886 FR 61858 (November 08, 2021).

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

- Individuals seeking information regarding access to and contesting of VA records may write, call, or visit the nearest VA regional office. See VA SORN Compensation, Pension, Education and Employment Records-VA, SORN 58VA21/22/2886 (November 08, 2021).

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 individual 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 files. Furthermore, this document and the SORN provide the point of contact for members of the public who have questions or concerns about applications and files.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system.

- Applicants must request access via VA FORM 20-8824E or, electronically, using Common Security Services' Common Security Employee Manager (CSEM). Applicants must also complete mandatory VA Security and Privacy Awareness training, complete/sign User Access Request Form, and review, acknowledge, and electronically sign the VA Rules of Behavior.

- More information regarding this process may be found here: Common Security Services (CSS) - Office of Business Integration (va.gov)

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?

- NARA and DoD User's may gain access to the system. Users must follow the process described in 8.1a, above. The VA OBI establishes the criteria for what PII may be shared.

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.

- BEP's CSS provides over 150 different roles to meet the needs of customer applications

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.

- OIT 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.
- 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, ISSO, 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.

8.3 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 ROB or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. VA employees and 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). The rules are included as part of the security awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the Rules, the user must reaffirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. All VA employees must complete annual Privacy and Security training. 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 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, ISSO, 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.

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

8.4a If Yes, provide:

The documentation dates, provided below, are for the combined VBA Corporate Infrastructure (CRP-BEP) authorization package. BEP is in the process of establishing its own ATO.

1. *The Security Plan Status:* Current
2. *The System Security Plan Status Date:* 06/28/23
3. *The Authorization Status:* Authorized
4. *The Authorization Date:* 06/02/23
5. *The Authorization Termination Date:* 10/04/23
6. *The Risk Review Completion Date:* 06/27/23
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)*

- BEP does not currently utilize 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.*

- N/A

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

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

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

- N/A

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

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

- N/A

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

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

- N/A

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

ID	Privacy Controls
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment

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

Signature of Responsible Officials

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

JEAN-CLAUDE WICKS

Digitally signed by JEAN-CLAUDE WICKS
Date: 2023.08.04 04:57:00 -06'00'

Privacy Officer, Jean-Claude Wicks

TAMER AHMED

Digitally signed by TAMER AHMED
Date: 2023.08.04 07:08:59 -04'00'

Information System Security Officer, Tamer Ahmed

Derolyn D. Dozier 192409

Digitally signed by Derolyn D. Dozier 192409
Date: 2023.08.04 07:35:20 -05'00'

Information System Owner, Derolyn Dozier

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).

- VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records— VA'' (58VA21/22/28)
    - https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

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