Privacy Impact Assessment for the VA IT System called:

Enterprise Management Payment Workload & Reporting (eMPWR-VA)

Office of Information Technology (OIT)

Date PIA submitted for review:

July 12, 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	Jeff Ivy	Jeffrey.Ivy@va.gov	813-980-2382

Abstract

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

Enterprise Management of Payment Workflow and Reports (eMPWR- VA) is a modernization of the existing Veterans Service Network (VETSNET) Finance and Accounting System (FAS) and facilitates payment processing for the entire C&P and Educational claims process. It manages the individual beneficiary ledgers and the VA agency ledgers and interacts with systems at the US Treasury to ensure proper payment processing. The system receives awards information by reading the data from the VBA Corporate Database (CorpDB), processes the financial transactions, and sends payment info back to CorpDB – which in turn sends info to both the U.S. Treasury and the VA Financial Management System (FMS) for recording in the agency ledgers. eMPWR-VA is migrating from an Oracle VA Enterprise Cloud Amazon Web Services (VAEC-AWS) GovCloud and is under the Benefits Integration Platform (BIP) Assessing authority to operate (ATO).

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 Management of Payment Workflow and Reports (eMPWR- VA) serves the Office of Financial Management (OFM) The system is being built and managed by the Office of Information Technology (OIT).

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

eMPWR facilitates payment processing for the entire Compensation & Pension (C&P) and Educational claims process. It manages the individual beneficiary ledgers and the VA agency ledgers and interacts with systems at the US Treasury to ensure proper payment processing.

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

Office of Financial Management (OFM).

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 system uses PII and Financial information, including first name, last name, SSN, date of birth, personal payment mailing address, work address, zip code, personal phone number, work phone number financial account information, health insurance beneficiary numbers, medical conditions for which awards have been made and service history to ensure payments are accurate. The expected number of individuals and vendors whose information is stored in the system is approximately 4 million.

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

eMPWR manages the individual beneficiary ledgers and the VA agency ledgers to ensure proper payment processing. The system receives awards information by reading the data from the VBA Corporate Database (CorpDB), processes the financial transactions, and sends payment info back to CorpDB – which in turn sends info to both the U.S. Treasury and the VA Financial Management System (FMS) for recording in the agency ledgers

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

Based on the data received, eMPWR will calculate payments due to veterans after the addition of Proceed Balances and deduction of Receivable Balances. In doing so, eMPWR will support the following functions necessary for proper General Ledger Accounting:

- Payable Benefits including Retroactive and Recurring Payments
- Modifying and checking proceeds balances
- Modifying and checking receivable balances
- Generating payments

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

The system integrates and makes use of the VBA Corporate Database which tracks Veterans Claims and Awards using a unique File Number, which is often a SSN. In addition, the system uses SSN to ensure that payment information is properly transferred to the U.S. Treasury. eMPWR operates in a single Region of the VA Enterprise Cloud (VAEC) in Amazon Web Services (AWS) GovCloud, deployed across three Availability Zones.

3. Legal Authority and SORN

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

eMPWR has the legal authority to use the SSN by Legal Authority – Privacy Act of 1974; US Code title 5 USC section 301 title 38 section 1705,1717, 2306-2308 & Title 38, US Code section 7301(a) and Executive Order 939

This SORN can be found online at 2021-24372.pdf (govinfo.gov)

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, SORN requirements are handled via the eMPWR system. eMPWR leverages the VAEC Cloud Service Provider (CSP) AWS GovCloud, which is FEDRAMP approved, under the BIP Assessing ATO. Per the approval of the Deputy Assistant Secretary, Enterprise Program Management Office (EPMO) [the VA Authorizing Official (AO)], BIP has an ATO for one calendar year, effective January 21, 2021. VA Business Stakeholders of the BIP minor applications have ownership rights over data.Security and privacy data held by a cloud provider is still required to meet the requirements under the privacy act. Federal agencies are required to identify and assess the risk to their PII, and to ensure security controls are implemented to provide adequate safeguards. Section C MM. of the contract references OMB Memorandum "Security Authorization of Information Systems in Cloud Computing Environments" FedRAMP Policy Memorandum.

D. System Changes

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

Completion of this PIA will not result in circumstances requiring changes to business processes.

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)

- Place of birth
- Biometric records
- Criminal history
- Participant number
- Employment history (not PII)
- Work address (not PII)
- Work phone number (not PII)
- Education (not PII)

PII Mapping of Components (Servers/Database)

eMPWR consists of one key component (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by eMPWR 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
CorpDB	Yes	Yes	education, financial transactions, medical history, and criminal or employment history, first name, last name, social security number, date and place of birth, mother's maiden name, biometric records	To further improve performance, eMPWR will implement an OnLine Analytical Processing (OLAP) database.	Logs for AWS Data Migration Service (DMS) are stored initially in Amazon CloudWatch, a monitoring service for all AWS services. The logs are segregated by service instance, so the logs specific to eMPWR data replication are not co-mingled with logs rom other applications using AWS DMS. The BIP Platform provides several

					log aggregation tools that can pull data from Amazon CloudWatch and coordinate it with eMPWR system logs and monitoring dashboards. These capabilities will provide for a single administrative and operational capability across the eMPWR application.

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

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

The central data layer is the Corp DB, which hosts the financial data used by eMPWR. eMPWR-VA is the primary user for Financial Data in CorpDB (within the FA, FA Batch, and FA Reporting Schemas).

1.2b Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

The Transactional Data Store for eMPWR-VA will be the CorpDB. While there may be performance and code simplicity advantages to moving eMPWR-VA transactional data storage to its own database, OIT leadership made the decision to leave financial data in CorpDB to avoid potential issues with data synchronization and increased management of data across different databases.

That said, the eMPWR-VA team desires to work with the CorpDB Data Architecture (DA) and Database Administration (DBA) groups to make several performance improvements to CorpDB. These improvements include:

- Improving the use of table column indexes to increase performance.
- Support DA efforts to archive historical data both in the data tables and their associated journal tables to again reduce the amount of data involved in data processing.

- Implementing materialized views for reports and during batch processing that reduce the overall number of queries necessary to generate reports and process transactions.

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

eMPWR-VA does not create 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?

To replicate data from CorpDB to the Analytical Data Platform, AWS DMS (Amazon Web Services Database Migration Service) will use SSL/TLS encrypted communications over Port 1 SQLNet connectivity over Port 15239 (or other port as required by CorpDB). Traffic between the AWS DMS instance and the ADS instance will likewise be encrypted using SSL/TLS. In addition, AWS DMS will use a specialized database account on both CorpDB and the ADS with specific grants necessary for replication. The credentials for these accounts will be rotated in conformance with VA elevated privilege account policies and the credentials will be stored securely in the BIP Platform instance of Vault.

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.

eMPWR-VA does not use paper forms or surveys to collect data.

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.

AWS DMS is a cloud-based data replication and synchronization solution that allows for uni- or bi-directional synchronization of data between two heterogenous database instances. AWS DMS is hosted on the largest data processing cloud in the world. If a local failure prevents AWS DMS from completing, the workload is automatically shifted to a secondary availability zone for processing, resulting in very little downtime (typically a few seconds or less). More advanced architectures can

be created to shift loads across geographic regions within seconds to minutes to handle geographically widespread outages

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.

eMPWR-VA does not use commercial aggregators to check the accuracy of the data.

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

eMPWR has the legal authority to use the SSN by Legal Authority – Privacy Act of 1974; US Code title 5 USC section 301 title 38 section 1705,1717, 2306-2308 & Title 38, US Code section 7301(a) and Executive Order 939. We are not aware of any additional agreements beyond VETSNET's existing PIA. Please refer to Appendix A-6.1.

This SORN can be found online at 2021-24372.pdf (govinfo.gov)

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: Information could be breached or accidentally released to inappropriate parties or the public.

Mitigation: eMPWR-VA will provide secure network interface access to VA data for authorized users and systems to support VBA financial management business processes. eMPWR-VA will be securely connected to the required VA systems of record. eMPWR-VA connection to any VA data system will be reviewed and approved as part of the VA Solutions Design process and will be implemented following VA Security and SDLC policy. The VA trusted network can be accessed only through two-factor PIV authentication. eMPWR-VA will only be accessed from within the VA trusted network and accessed only through two-factor PIV authentication. IP address whitelisting in Salesforce will be set up to ensure the access is only available from the VA network and Salesforce integration with VA Active Directory will enforce two factor authentication and authorization for all Salesforce users. In addition, eMPWR-VA will make use of the CSS application established in the CorpDB environment to maintain and restrict eMPWR-VA specific security levels. Lastly, all of the Oracle database tables that support legacy FAS are journaled per standards that meet the standard audit processes.

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.

Please provide response here

- First name, Last name: Used as a participant identifier
- SSN: Used as a participant identifier
- Personal payment mailing address: Used to issue payment to participant
- Participant Number: Used to identify participant
- Zip code: Used to issue payment to participant
- Financial account information: Used to issue payment to participant

Below data elements are not stored in eMPWR, but are contained within external data sources that are integrated with eMPWR

- Health insurance beneficiary numbers
- Medical conditions
- Education
- Work address
- Personal phone number
- Work phone number
- Place of birth
- Mother's maiden name

- Biometric records
- Medical history
- Date of Birth
- Criminal history
- Employment history

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.

Data is not created in eMPWR.

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.

MuleSoft Anypoint Server is the bridge between the UI and the backing CorpDB. Requests arriving at MuleSoft will be validated for content, appropriateness of the request, and the authentication tokens of the end user for whom the request was made. Upon successful validation of the request, MuleSoft will send a SQL request to CorpDB using SQLNet protocol over port 1521 (or other port as configured by the CorpDB DBAs). Appropriate network security controls are already in place on the BIP Platform to allow traffic to securely move from the BIP Platform in VAEC to the CorpDB database.

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?

The SSN are encrypted in transition and not stored within eMPWR.

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

Yes, the SSN are encrypted in transition and not stored within eMPWR. The SSN come from the Corporate Database (CorpDB)

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

eMPWR was designed, developed, deployed, and is operated and maintained within the requirements of OMB Memoranda M-06-15 Safeguarding Personally Identifiable Information and M-06-16 Protection of Sensitive Agency Information. Specifically, the VA has designated the Deputy CIO as the Senior Agency Official for Privacy (SAOP), and eMPWR encrypts all data in transit, uses two factor authentications, time out functions, and event logging in accordance with VA6500 Rev 4.

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 PII/PHI, we need to submit a request ticket in JIRA to document such actions.

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

- Yes, all access control procedures are documented and uploaded into the following VA SharePoint page: https://dvagov.sharepoint.com/sites/OITDSOSPMBIAProductLine-Product-BIP-IA/Shared%20Documents/Forms/AllItems.aspx?ga=1&id=%2Fsites%2FOITDSOSPMBIAProductLine%2DProduct%2DBIP%2DIA%2FShared%20Documents%2FProduct%20%2D%20BIP%20%2D%20IA%2FSOPs%2FMinor%20App%20SOPs%2FeMPWR&viewid=6eaed4f3%2Dfa76%2D44c8%2Db00d%2D4b4957fd0ade

- All employees with access to Veteran's information are required to complete the mandatory VA Privacy and Information Security Awareness training and Rules of Behavior annually.

- Disciplinary actions, depending on the severity of the offense, include counseling, loss of access, suspension and possibly termination.

- 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 twofactor authentication. The user's ID limits the access to only the information required to enable the user to complete their job.

2.4c Does access require manager approval?

Yes, anytime we need to access PII/PHI, we need to submit a request ticket in JIRA to document such actions.

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

Individual users are given access to Veteran's data through the issuance of a user ID and password and using a Personal Identity Verification (PIV) card. This ensures the identity of the user by requiring two factor authentication. The user's ID limits the access to only the information required to enable the user to complete their job

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

The security controls cover 15 security areas for protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security areas include access control; audit and accountability; security assessment and authorization; configuration management; contingency planning; identification and authentication; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. The RLS application team has implemented the required security controls based on the tailoring guidance of NIST Special Publication 800-53 and VA directives or handbooks. VA Records Management Policy; VA Handbook 6500, Rules of Behavior (ROB); and VA 6502.1, VA6502.3, and VA 6502.4 Privacy Policies govern how veterans' information is used, stored, and protected.

Section 3. Retention of Information

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

3.1 What information is retained?

*Identify and list all information collected from question 1.1 that is **retained** by the system.*
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal

eMPWR does not retain any of the PHI/PII information listed in section 1.1. The eMPWR retention policy is inherited by VETSNET, please refer to Appendix A-6.1for a copy of the retention language.

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.*

The corporate database remains the system of record. Records are maintained and disposed of in accordance with the records disposition authority approved by the Archivist of the United States. Records from this system that are needed for audit purposes will be disposed of 6 years after a user's account becomes inactive. Routine records will be disposed of when the agency determines they are no longer needed for administrative, legal, audit, or other operational purposes. These retention and disposal statements are pursuant to National Archives and Records Administration (NARA) General Records Schedules GRS 3.2, item 30 and GRS 3.2, item 31. Records are maintained and disposed of in accordance with the records from this system, 7 years. National Archives and Records Administration (NARA) guidelines as stated in RCS 10-1 records retention schedule requires retention for 75 years. The data retention period has been approved by NARA and is processed according to the following:

- General Records Schedule: General Records Schedules (GRS) | National Archives or https://www.archives.gov/records-mgmt/grs.html

Refer to the connected applications security/privacy documentation to review application processes for information retention and destruction schedules.

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?

Records are maintained and disposed of in accordance with the records disposition authority approved by the Archivist of the United States.

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

eMPWR-VA follows the VA retention period has been approved by NARA and is processed according to the
following:

- General Records Schedule: General Records Schedules (GRS) | National Archives or https://www.archives.gov/records-mgmt/grs.html

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.

eMPWR-VA records are not destroyed every 7 years and records can be queried from system instantiation.

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.

PII collected by eMPWR is not used for research, training, or testing.

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 maintained could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being

unintentionally released or breached.

Mitigation: User access is not provided by eMPWR but by the VA ePAS process. The following are true of all VA information system users:

- All employees with access to Veteran's information are required to complete the mandatory VA Privacy and Information Security Awareness training and Rules of Behavior annually.
- Disciplinary actions, depending on the severity of the offense, include counseling, loss of access, suspension and possibly termination.
- 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. The user's ID limits the access to only the information required to enable the user to complete their job.

eMPWR does not create, adjust, or make data in any way.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Veterans Benefits Management System (VBMS)	Provides PII	Social Security Number, Benefits Information	Document uploads via Application Programming Interface (API)
Benefits Integration Platform (BIP)/ Mulesoft	Provides API and data services that transmits PII from backend to front end	Social Security Number, Benefits Information	Data packages moving from Salesforce to Application Programming Interface (API) to database
Veteran Health Administration VA **Financial Management System (FMS)**	Provides PII	Social Security Number, Benefits Information, Participant number, financial account information	Application Programming Interface (API) with FMS
Debt Management Center (DMC) **Computer Access Request System (CARS)**	Provides Financial information	financial account information • first name • last name • SSN • date of birth	Application Programming Interface (API) with CARS

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
Veterans Benefits Management System (VBMS)	Provides PII	Social Security Number, Benefits Information	Document uploads via Application Programming Interface (API)
Benefits Integration Platform (BIP)/ Mulesoft	Provides API and data services that transmits PII from backend to front end	Social Security Number, Benefits Information	Data packages moving from Salesforce to Application Programming Interface (API) to database
Veteran Health Administration **Master Person Index (MPI)**	Provides PII	• first name • last name • SSN • date of birth • personal payment mailing • address • place of birth • mother's maiden name • biometric records • medical history • criminal history • Participant Number • employment history • work address • zip code • personal phone number • work phone number • financial account information • health insurance	Internal database connection

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (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 privacy risk associated with maintaining SPI is that this data may be disclosed to individuals who do not require access, which would increase the risk of the information being misused

Mitigation: Safeguards are implemented to ensure data is not sent to unauthorized VA employees, including employee security and privacy training, and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized for 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***
US Treasury	To pay the beneficiaries	SSN, name, and Physical address/ACH payment address information	DoT Fiscal Service VA System BDN VETSET ISA MOA; SORN Routine Use # 24	ConnectDirect secure file transfer
Prudential	To send/receive life insurance information to beneficiaries	Social security number, name	ISA MOA between HITC and Prudential Insurance Company of America; Prudential Group Policy 32000	ConnectDirect secure file transfer

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

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

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

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

Follow the format below:

Privacy Risk: No open risks concerning sharing, hacking, or phishing

Mitigation: No open risks concerning sharing, hacking, or phishing

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.

58VA21/22/28 (November 8, 2021) Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA. This SORN can be found online at 2021-24372.pdf (govinfo.gov) which includes a notice to the public of reasons for collection and types of records retained.

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

58VA21/22/28 (November 8, 2021) Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA. This SORN can be found online at 2021-24372.pdf (govinfo.gov)

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.

58VA21/22/28 (November 8, 2021) Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA. This SORN can be found online at 2021-24372.pdf (govinfo.gov) which includes a notice to the public of reasons for collection and types of records retained.

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.

Responding to collection is voluntary; however, if information is not provided; then benefits may be denied.

6.3 Do individuals have the right to consent to 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.

Individuals do not have the right to consent to uses of the information that do not fall within the Routine Uses as codified within the System of Record Notice (SORN)

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: There is a risk that members of the public may not know that the eMPWR system exists within the Department of Veterans Affairs.

Mitigation: The VA mitigates this risk by having veterans and other beneficiaries contact their supporting VA regional office or VHA center to learn how to access, correct, or contest their information. eMPWR receives information from other systems therefore veterans instead would have to go through the source system's protocols to correcting the data.

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.***

Members of the public are not allowed access to eMPWR. However, under the Privacy Act of 1974 everyone whom the government retains records are is entitled to a copy of those records. SORN 58VA21/22/28 (November 8, 2021) Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA. This SORN can be found online at Https://www.govinfo.gov/content/pkg/FR-2012-07-19/pdf/2012-17507.pdf which outlines the process for FOIA and Privacy Act Requests.

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).

eMPWR-VA is not exempt.

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.

eMPWR-VA 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.

58VA21/22/28 (November 8, 2021) Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA. This SORN can be found online at Https://www.govinfo.gov/content/pkg/FR-2012-07-19/pdf/2012-17507.pdf which outlines the process for correcting inaccurate or erroneous information.

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.

58VA21/22/28 (November 8, 2021) Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA. This SORN can be found online at 2021-24372.pdf (govinfo.gov) which outlines the process for correcting inaccurate or erroneous information. Notification of corrections is made once the request has been processed.

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 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 and other beneficiaries may contact their supporting VA regional office or VHA center to learn how to access, correct, or contest their information. eMPWR receives information from other systems therefore veterans instead would have to go through the source system's protocols to correcting the data.

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: At this time, we do not see any risks as the system complies with VA policy and multiple authentication and authorization policies, processes and technologies have been implemented to further secure the system.

Mitigation: N/A

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.

The first time a user accesses eMPWR, the Salesforce Authentication and Authorization process provides eMPWR-VA with their federated user ID (a properly registered and verified email address). However, CorpDB and the roles and security systems that control access to specific records require the transfer and inspection of a user's network ID and their participant ID from the participants table in CorpDB. The process of mapping between the three is a slow process, as it cannot make use of existing indexes in CorpDB. To prevent this from being a problem, on the first login, the system will query for the information via a First-Time-Login API implemented in MuleSoft. This API will return both the network ID and the participant ID for the user, which will be added to the user's Salesforce User Object. In subsequent logins, when the participant ID and network ID are already recorded in Salesforce, the system can simply reuse the existing information to fetch their default station, other stations, sensitivity level, and roles on a station-by-station basis.

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?

Some users are assigned to more than one station. In this case, they will have the ability to select a different station from their default in which to process transactions. Should they do so, their roles may also change. Access is requested per VA 6500 policies utilizing Electronic Permission Access System (ePAS). Users submit access requests based on need to know and job duties. Supervisor, ISO

and OI&T approval must be obtained prior to access granted. These requests are submitted for VA employees, contractors and all outside agency requests and are processed through the appropriate approval processes. Once access is granted, individuals can log into the system(s) through dual authentication, i.e., a PIV card with a complex password combination (two-factor authentication is enforced). Once inside the system, individuals are authorized to access information on a need-to-know basis.

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.

eMPWR-VA has five primary categories of users, which are identified and defined in the following sections.

1. Accountants: Accountant users perform and monitor accounting related transactions. They manage unassociated balances, journal transactions and miscellaneous accounting. Finance users/accountants work in Stations 201 and 282 (Hines Finance). The types of transactions they work on:
    a. Unassociated transactions in order to clear Unassociated accounts.
    b. Miscellaneous accounting transactions for benefit programs managed by CorpDB.
    c. Journal Vouchers adjusting transactions for the benefit program ledgers managed by CorpDB. BID 1002AK eMPWR-VA System Design Document April 07, 2023 Task Order No: 36C10B21N10070021 –14– Benefits Integrated Delivery These users will use both canned and custom reports from eMPWR-VA to ensure that proper accounting is performed so that payments disbursed to Veterans and their beneficiaries can be certified as legal, proper, and correct.
2. Finance clerks: Finance clerks create and authorize business transactions and monitor the beneficiary's account activity. They process payments directly from eMPWR-VA, create and adjust receivables, create transactions to establish or adjust deductions from payments as well as manage accountable balances. These users will need to view specific canned reports and dashboards in support of their role.
3. Finance Manager: Finance Managers use eMPWR-VA to validate batch processes and to identify errors in payment files. They require access to Online Analytical Processing (OLTP), canned and ad-hoc reports, and dynamic interfaces to manage the overall VBA financial accounting process. Their need for ad-hoc reporting is related to regularly received special requests to address Freedom of Information Act (FOIA) inquiries, management decisions, and internal and external audit and oversight groups (e.g., Inspector General (IG), Office of Management and Budget (OMB), Congressional requests, etc.).
4. Production Support: Production Support staff provide daily support in the CorpDB transactional environment, support the batch processes, monitor the health of batch jobs, provide real-time technical support as needed to ensure that all batch jobs complete successfully, support reporting and ensure that data replication runs, and all canned reports are generated by 5 a.m. CT.
5. System Administrators: While the system administrators do not directly interact with the eMPWR-VA system, they are necessary support staff for managing the scheduling of batch jobs, as well as providing operational and security management support on the infrastructure that houses the eMPWR-VA system.

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.

The eMPWR program contractors who provide support to the system are required to complete a Moderate Background Investigation (MBI), complete annual VA Privacy and Information Security and Roles of Behavior training via the VA's Talent Management System TMS. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access. VA contract employee system/application access is verified through VA Contract Officers Representative (COR) before access is granted to any contractor.

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.

Users are required to complete information system security training activities including annual security awareness training, Privacy training and specific information system security training. The training records are retained for 7 years. This documentation and monitoring are performed using the Talent Management System (TMS).

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

8.4a If Yes, provide:

1. *The Security Plan Status:* An A&A has not been completed.
2. *The System Security Plan Status Date:* An A&A has not been completed.
3. *The Authorization Status:* An A&A has not been completed.
4. *The Authorization Date:* An A&A has not been completed.
5. *The Authorization Termination Date:* An A&A has not been completed.
6. *The Risk Review Completion Date:* An A&A has not been completed.
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* An A&A has not been completed.

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

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

The BIP Assessing (under which eMPWR is a minor application) Authority to Operate (ATO) with Conditions was granted on January 17, 2023 and lasts until January 17, 2024. The FIPS 199 classification of the system is HIGH.

Section 9 – Technology Usage

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

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

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

VA Enterprise Cloud (VAEC) Amazon Web Services (AWS) govcloud-west service

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.*

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.

9.3 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.

9.4 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).

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

JEAN-CLAUDE WICKS

Digitally signed by JEAN-CLAUDE WICKS
Date: 2023.07.25 04:41:11 -06'00'

Privacy Officer, Jean-Claude Wicks

JOSEPH FACCIOLLI

Digitally signed by JOSEPH FACCIOLLI
Date: 2023.07.25 09:42:20 -04'00'

Information System Security Officer, Joseph Facciolli

Jeffrey L. IVY 246254

Digitally signed by Jeffrey L. IVY 246254
Date: 2023.07.25 09:50:14 -04'00'

Information System Owner, Jeff Ivy

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).

As referenced in Section 1 and 3 of this eMPWR-VA PIA, approved VETSNET PIA description is provided as an appendix below. Also the full document of the VETSNET PIA can be provided upon request by emailing PIASupport@va.gov.

VETSNET Section 1. Characterization of the Information

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

- Title 10 U.S.C. chapters 106a, 510,1606 and 1607 and Title 38, U.S.C. Section 501(a) and Chapters 11, 13, 15,18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51,53, and 55 provide the legal authority for operating VETSNET. VA gathers or creates these records in order to enable it to administer statutory benefits programs to Veterans, Service members, reservists, and their spouses, surviving spouses, and dependents, who file claims for a wide variety of Federal Veteran's benefits administered by VA.''
- Presidential Review Directive 5, A National Obligation – Planning for Health Preparedness for and Readjustment of the Military, Veterans, and Their Families after Future Deployments, August 1998
- Per SORN 24VA10P2 – Patient Medical Records Title 38, United States Code, Section 501(b) and 304.
- Memorandum of Understanding Between the Department of Defense (DOD) and the Department of Veterans Affairs (VA) for Sharing Personal Information, March 13, 2014

VETSNET PIA 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

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

3.2 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.

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

Compensation, pension, and vocational rehabilitation claims folders are retained at the servicing regional office until they are inactive for three years, after which they are transferred to the Records Management Center (RMC) for the life of the Veteran. Official legal documents (e.g., birth certificates, marriage licenses) are returned to the claimant after copies are made for the

claimant's file. At the death of the veteran, these records are sent to the Federal Records Center (FRC), and maintained by the National Archives and Records Administration (NARA) in accordance with NARA policy. Some claims folders are electronically imaged; in which case, the electronic folder is maintained in the same manner as the claims folder. Once a file is electronically imaged and accepted by VBA, its paper contents (with the exception of documents that are the official property of the Department of Defense, and official legal documents), are destroyed in accordance with Records Control Schedule VB–1 Part 1 Section XIII, as authorized by NARA. Documents that are the property of the Department of Defense are either stored at the RMC, or transferred to NARA and maintained in accordance with NARA policy.

Vocational Rehabilitation counseling records are maintained until the exhaustion of a Veteran's maximum entitlement or upon the exceeding of a Veteran's delimiting date of eligibility (generally, ten or twelve years from discharge or release from active duty), whichever occurs first, and then destroyed. Automated storage media containing temporary working information are retained until a claim is decided, and then destroyed. All other automated storage media are retained and disposed of in accordance with disposition authorization approved by NARA. Education electronic folders are retained at the servicing Regional Processing Office. Education folders may be destroyed in accordance with the times set forth in the Veterans Benefits Administration Records Management, Records Control Schedule VB–1, Part 1, Section VII, as authorized by NARA. Employee productivity records are maintained for two years after which they are destroyed by shredding or burning. File information for U.S. Department of Housing and Urban Development (HUD) Credit Alert System (CAIVRS) is provided to HUD by the VA on magnetic tape. After information from the tapes has been read into the computer the tapes are returned to VA for updating. HUD does not keep separate copies of the tapes.

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