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:

1/29/2021

System Contacts:

<table>
<thead>
<tr>
<th>Title</th>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Gwendolyn Smith</td>
<td><a href="mailto:gwendolyn.smith1@va.gov">gwendolyn.smith1@va.gov</a></td>
<td>202-632-8928</td>
</tr>
<tr>
<td>Information System Security Officer</td>
<td>Joseph Facciolli</td>
<td><a href="mailto:Joseph.Facciolli@va.gov">Joseph.Facciolli@va.gov</a></td>
<td>(215) 842-2000 x2012</td>
</tr>
<tr>
<td>Information System Owner</td>
<td>Jeff Ivy</td>
<td><a href="mailto:Jeffrey.Ivy@va.gov">Jeffrey.Ivy@va.gov</a></td>
<td>813-980-2382</td>
</tr>
</tbody>
</table>
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 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:

- The IT system name and the name of the program office that owns the IT system.
- The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.
- The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
- If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?
- A general description of the information in the IT system.
- Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.
- 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.
- A citation of the legal authority to operate the IT system.
- Whether the completion of this PIA will result in circumstances that require changes to business processes
- Whether the completion of this PIA could potentially result in technology changes
- If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval?
- Does the system use cloud technology?  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.
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).

eMPWR 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 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.

eMPWR is a national system.

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.

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, and
- Generating payments.

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.

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

Completion of this PIA is not anticipated to result in technology changes.

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.

Veterans Benefits Administration (VBA) will have rights over the 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.

The contract outlines Management of Security and Privacy Incidents IAW VA Handbook 6500.2. Based on determinations of independent risk analysis, the Contractor shall be responsible for paying to VA liquidated damages for affected individuals to cover the cost of providing credit protection services to affected individuals. Would the reputation of the CSP or its customers (VA) be affected? Yes. CSPs are required to meet the same requirements when operating on behalf of the federal government.

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://www.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.

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 (first and last)
- 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 Account Information
- Health Insurance Beneficiary Numbers
- Account numbers
- Certificate/License numbers
- Vehicle License Plate Number
- Internet Protocol (IP) Address Numbers
- Current Medications
- Previous Medical Records
- Race/Ethnicity
- Tax Identification Number
- Medical Record Number
- Other Unique Identifying Number (list below)

The system uses PII including work address, zip code, work phone number, medical conditions for which awards have been made and service history to ensure payments are accurate.

PII Mapping of Components

eMPWR consists of one key component. 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.

PII Mapped to Components

<table>
<thead>
<tr>
<th>Components of the information system (servers) collecting/storing PII</th>
<th>Does this system collect PII? (Yes/No)</th>
<th>Does this system store PII? (Yes/No)</th>
<th>Type of PII (SSN, DOB, etc.)</th>
<th>Reason for Collection/Storage of PII</th>
<th>Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analytical Data Store - AWS RDS Oracle database</td>
<td>Yes</td>
<td>Yes</td>
<td>first name, last name, SSN, date of birth, personal payment mailing address,</td>
<td>To further improve performance, eMPWR will implement an OnLine Analytical Processing (OLAP)</td>
<td>Logs for AWS Data Migration Service (DMS) are stored initially in Amazon CloudWatch, a monitoring service for all</td>
</tr>
<tr>
<td>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</td>
<td>database. The structure for this database will be optimized for reporting to minimize the number of computationally expensive join operations needed to produce each report. In addition, only the data required to produce the reports required each night will be transferred from CorpDB to the data store. This will ensure that the data involved in reporting is the minimum set necessary for reporting. The transfer of data from CorpDB to the Analytical Data Store will be conducted via AWS Data Migration Service (DMS). AWS services. The logs are segregated by service instance, so the logs specific to eMPWR data replication are not co-mingled with logs from 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.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1.2 What are the sources of the information in the system?

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?

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 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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).

The Transactional Data Store for eMPWR-VA will be the CorpDB. Implementation of table partitioning is planned to improve FAS transactional performance. 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:

- Using database partitioning to partition the largest tables in the database in a way that decreases the number of records that must be processed during both batch and UI processing.
- Improving the use of table column indexes and partition 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 during batch processing that reduce the overall number of queries necessary to process transactions.

1.3 How is the information collected?

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 technology used in the storage or transmission of information in identifiable form?

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.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

To replicate data from CorpDB to the Analytical Data Platform, AWS DMS 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.

1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?
Include a statement of why the particular SPI is collected, maintained, used, or disseminated in the system is necessary to the program’s or agency’s mission. Merely stating the general purpose of the system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

If the system collects, uses, disseminates, or maintains publicly available or commercial data, include a discussion of why commercial data is relevant and necessary to the system’s purpose. This question is related to privacy control AP-2, Purpose Specification.

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.

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, and
- Generating payments.

1.5 How will the information be checked for accuracy? How often will it be checked?

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.

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. This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

AWS DMS is a cloud-based data replication and synchronization solution that allows for uni- or bidirectional 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.
1.6 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.

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.

1.7 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.

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 information were breached or accidentally released to inappropriate parties or the public, it could result in potential personal and/or emotional harm to the friends/relatives of the individuals whose information is contained in the system.

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.

- First name, Last name: Used as a participant identifier
- SSN: Used as a participant identifier
- Date of Birth: Used to identify participant age and confirm patient identity
- Personal payment mailing address: Used to validate participant place of residence
- Work address: Used to identify participant place of employment
- Personal phone number: Used to identify participant and contact participant
- Work phone number: Used to identify participant place of employment and contact number
- Financial account information: Used to identify participant financial account information need to for benefits
- Health insurance beneficiary numbers: Used to communicate and bill third party health care plans
- Medical conditions: Used to quality the participant for which awards have been made and service history to ensure payments are accurate.

2.2 What types of tools are used to analyze data and what type of data may be produced?

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.

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.
This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

Data is not created in eMPWR.
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 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

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.

Access to the PII is determined by authentication and authorization mechanisms implemented in the eMPWR system. The PIA is maintained by the Project Manager and can be obtained through the Privacy Office.
• 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.

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

The eMPWR retention policy is inherited by VETSNET, Please refer to Appendix A-6.1 for 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.

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

No input for this section because eMPWR-VA is SORN is not applicable

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 Privacy 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.

VETSNET remain the system of record. Please refer to the appendix for VETSNET PIA
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:

- Control Schedule 10-1 link for VHA: OFC
- Control Schedule VB-1, Part II Revised for VBA: https://www.benefits.va.gov/WARMS/topic-title38.asp
- Archives and Records Administration: www.nara.gov

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)? If so please indicate the name of the records retention schedule.

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner.

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

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

- Control Schedule 10-1 link for VHA: OFC
- Control Schedule VB-1, Part II Revised for VBA: https://www.benefits.va.gov/WARMS/topic-title38.asp
- Archives and Records Administration: www.nara.gov

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the 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

Electronic media sanitization, when the records are authorized for destruction (or upon system decommission), will be carried out in accordance with VA 6500.1 HB Electronic Media Sanitization.
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. Have policies and procedures been developed to minimize the use of PII 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.

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. NOTE: Question 5 on Privacy Threshold Analysis should be used to answer this question.

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?

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

<table>
<thead>
<tr>
<th>List the Program Office or IT System information is shared/received with</th>
<th>List the purpose of the information being shared/received with the specified program office or IT system</th>
<th>List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>CorpDB</td>
<td>CorpDB is the data source for all eMPWR data.</td>
<td>education, financial transactions, medical history, and criminal or employment history; (ii) Information that can be used to distinguish or trace the individual’s identity,</td>
<td>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</td>
</tr>
<tr>
<td><strong>List the Program Office or IT System information is shared/received with</strong></td>
<td><strong>List the purpose of the information being shared/received with the specified program office or IT system</strong></td>
<td><strong>List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system</strong></td>
<td><strong>Describe the method of transmittal</strong></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td></td>
<td></td>
<td>including first name, last name, social security number, date and place of birth, mother’s maiden name, biometric records or any other personal information which is linked or linkable to an individual</td>
<td>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. To replicate data from CorpDB to the Analytical Data Platform, AWS DMS 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.</td>
</tr>
</tbody>
</table>

**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.
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:** This question is #7 in the Privacy Threshold Analysis.

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

<table>
<thead>
<tr>
<th>List External Program Office or IT System</th>
<th>List the purpose of information being shared /</th>
<th>List the specific data element types such as</th>
<th>List the legal authority, binding</th>
<th>List the method of transmission and the</th>
</tr>
</thead>
</table>

Version Date: January 2, 2019
Page 16 of 23
<table>
<thead>
<tr>
<th>information is shared/received with</th>
<th>received / transmitted with the specified program office or IT system</th>
<th>PHI/PHI that are shared/received with the Program or IT system</th>
<th>agreement, SORN routine use, etc. that permit external sharing (can be more than one)</th>
<th>measures in place to secure data</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

eMPWR does not share information with any programs outside the VA.

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

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.

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:  N/A eMPWR does not share information with systems outside of the VA
Mitigation:  N/A

Section 6. Notice
The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an appendix. (A 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?
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. If notice was provided in the Federal Register, provide the citation.

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

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 question is 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.

This Privacy Impact Assessment (PIA) serves as notice. As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs “after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means.”

The system of record is the legacy system FAS and CorpDB. eMPWR-VA is a multiyear modernization effort which at this time duplicates a very small set of capabilities from FAS. The rights to this financial information and the actions taken on this information are at the direction of the participant (Veteran or Veteran beneficiary) who has submitted a financial claim.

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

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 particular uses of the information? If so, how does the individual exercise the right?

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

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.
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 providing the public with two forms of notice that the system exists, as discussed in detail 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.

**Section 7. Access, Redress, and Correction**

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

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.

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).

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.

This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

Members of the public are not allowed access to eMPWR. An individual who wishes to determine whether a record is being maintained under his or her name or wishes to determine the contents of such records should submit a written request or apply in person to the VA facility where the records are located. For a directory of VA facilities and phone numbers by region, see https://www.benefits.va.gov/benefits/offices.asp.

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.

Under the jurisdiction of VHA, VHA Handbook 1605.1 Appendix D ‘Privacy and Release Information’, section 8 states the rights of the Veterans to amend to their records via submitting VA Form 10-5345a, Individual's Request For a Copy of Their Own Health Information, may be used as the written request requirement, which includes designated record sets, as provided in 38 CFR 1.579 and 45 CFR 164.526. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and is filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

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 are not notified if there is missing or inaccurate information in their record. An individual who wishes to determine whether a record is being maintained under his or her name or wishes to determine the contents of such records should submit a written request or apply in person to the VA facility where the records are located. Requests should contain the full name, address and telephone number of the individual making the inquiry. (Per 58VA21/22/28 SORN)

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

Example: Some projects allow users to directly access and correct/update their information online. This helps ensure data accuracy.

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.

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.

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?

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

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?

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.

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

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.
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.

Strict physical security control measures are enforced to ensure that disclosure to these individuals is also based on this same principle. By policy, VA file areas are locked after normal duty hours and the facilities are protected from outside access by the Federal Protective Service or other security personnel.

OIT documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and retains individual training records for 7 years. This documentation and monitoring is performed through the use of the VA’s Talent Management System (TMS).

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 or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII.

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Yes, 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?

*If Yes, provide:*

1. The date the Authority to Operate (ATO) was granted,
2. Whether it was a full ATO or ATO with Conditions,
3. The amount of time the ATO was granted for, and
4. The FIPS 199 classification of the system (LOW/MODERATE/HIGH).

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

*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 21, 2021 and lasts until January 20, 2022. The FIPS 199 classification of the system is HIGH.
### Section 9. References

Summary of Privacy Controls by Family

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

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

Gwendolyn Smith 104878
Digitally signed by Gwendolyn Smith 104878
Date: 2021.02.03 10:38:56 -05'00'

Privacy Officer, Gwendolyn Smith

Joseph Facciolli 148552
Digitally signed by Joseph Facciolli 148552
Date: 2021.02.01 18:04:04 -05'00'

Information System Security Officer, Joseph Facciolli

Jeffrey L. IVY 246254
Digitally signed by Jeffrey L. IVY 246254
Date: 2021.01.29 17:50:36 -05'00'

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.”


- 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.