Privacy Impact Assessment for the VA IT System called:

Paper Mail Conversion and Management Services (PMCMS)

Veterans Benefits Administration (VBA)

Office of Business Integration

eMASS ID # 0185

Date PIA submitted for review:

06/16/2025

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Marvis Harvey	Marvis.Harvey@va.gov	202-461-8401
Information System Security Officer (ISSO)	Roger Carroll	Roger.Carroll2@va.gov	203-768-1066
Information System Owner	John Clark	John.Clark7@va.gov	708-830-3616

Abstract

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

(PMCMS) processes Personally Identifying Information (PII) and Personal Health Information (PHI/ePHI). Mail shipments of Veterans' physical documents are received at the scan vendor facility/facilities where they are prepared for scanning. Prepared documents are scanned and processed by VBA PMCMS as e-documents. This reduces paperwork and processing time for Veterans' claims and increases the ease and speed of access to their records. Hardcopy documents are held after scanning only as required to allow for review and any necessary re-scanning (to ensure high quality images) and are promptly and securely returned to the Department of Veterans Affairs custody.

Overview

The overview is the most important section of the Privacy Impact Assessment (PIA). A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

1 General Description

A. What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?

The Paper Mail Conversion and Management Service (PMCMS) Centralized Mail Portal system is a proprietary system owned by Leidos and provided as a System as a Service (SaaS) to the Veterans Benefits Administration (VBA). Converted centralized mail images and metadata represent a significant strategic asset for VA regarding completing Veteran claims for compensation and other benefits. As such, the Government currently utilizes the PMCMS CM Portal to provide VA access to converted mail packets for manual and automated processing by VA and contracted resources.

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

PMCMS Centralized Mail Portal system is a proprietary system owned by Leidos and provided as a System as a Service (SaaS) to the Veterans Benefits Administration (VBA).

2. Information Collection and Sharing

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

As of June 2025, the PMCMS CM Portal system contains data for approximately 18.786 million Veterans. This data is collected to support Veteran and dependent claims for compensation and other benefits.

Check if Applicable	Demographic of individuals
☒	Veterans or Dependents
☐	VA Employees
☐	Clinical Trainees
☐	VA Contractors
☐	Members of the Public/Individuals
☐	Volunteers

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

The PMCMS CM Portal collects, scans, and disseminates to VBMS and maintains the data for claims adjudication and processing.

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

PMCMS sends a message to the VA Claims Evidence Adapter (VACEA), which was developed and is maintained by GovernmentCIO. VACEA retrieves documents directly from the PMCMS object store in the AWS S3 storage in AWS GovCloud and in turn transmits the data and documents to VBMS via the Claims Evidence API.

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

Yes.

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

The PMCMS CM Portal is a cloud-based system hosted in the AWS GovCloud. The system is deployed to a single VPC across multiple subnets to separate front-end and back-end services. The PMCMS CM Portal is a primarily containerized, serverless, microservices architecture with only a few virtual machines hosting services for database, scanning vendor interfaces, and management/systems administration function. Leidos

retains responsibility for the safeguarding of the data in our custody, while ownership of the data remains with the VA.

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

H. What is the citation of the legal authority?

The legal authority includes Title 20 Chapter IX Part 1001, and the authorization for operation of VBA PMCMS is VA Contract No. VA118-11-D-1000, and Title 38, United States Code, section 501(a) and Chapters 11, 13, 15, 18, 23,30, 31, 32, 34, 35, 36, 39, 51, 53, 55 VBAPMCMS.

I. What is the SORN?

58VA21/22/28 86 FR 61858: Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA (https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf).

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

PMCMS is not a system of record.

4. System Changes

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

☐ Yes
☒ No
if yes, <<ADD ANSWER HERE>>

I. Will the technology changes impact information collection and sharing?

☒ Yes
☐ No
if yes, The change is that rather than submitting the data DIRECTLY to the system of record (VBMS), PMCMS transmits the data through and by the Government CIO VA Claims Evidence (VACE) Adapter (VACEA), which is owned and operated by Government CIO.

Section 1. Characterization of the Information

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

1.1 Information collected, used, disseminated, created, or maintained in the system.

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (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. It must also match the information provided in question 3.4 of the PTA.

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

- ☒ Name
- ☒ **Full** Social Security Number
- ☐ **Partial** 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[1]
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☐ Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☐ Sex
- ☒ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☐ Date of Death
- ☐ Business Email Address
- ☐ Electronic Data Interchange Personal Identifier (EDIPI)
- ☒ Other Data Elements (List Below)

Other PII/PHI data elements: Zip Code; VA File Number; Service-Related Disabilities

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

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

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?

PMCMS CM Portal receives information via conversion vendors who scan paper mail received from Veterans and send it via secure processes to the PMCMS CM Portal. PMCMS CM Portal also receives electronic Veteran data via conversion vendor Quick Submit electronic submission system.

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.

Scan vendors receive documents (printed and handwritten) from Veterans, Veteran family members, VSO, VBA Regional Offices, or third parties providing evidence in support of a claim. Documents may include paper, photographs, faxes, electronic source materials (eForms, eFax, CD/DVD, flash drives, microfilm, microfiche, and other alternate media (such as floppy disks). PMCMS receives this data in digitized format to facilitate and optimize the process to decide and pay Veteran claims.

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

The PMCMS CM Portal does not create any information.

1.3 Methods of information collection

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

PMCMS receives digitized claims documents via scan vendors. Scan vendors receive documents, convert them to PDFs, and transfer the PDF files and metadata to the PMCMS CM Portal system, via an existing, secure, automated, system-to-system process.

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

PMCMS CM Portal only receives electronic data and is not subject to the Paperwork Reduction Act.

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

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

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

Information processed by the PMCMS CM Portal consists of digitized forms and documents received in physical (analog) form and various digital formats. Any requirement to assess the accuracy of data provided to the source by a Veteran is beyond the operational requirements of the system. The accuracy of transmitted and stored data is ensured via the use of checksum/encryption standards (which meet FIPS 140-3 approval).

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

Please see answer to 1.4a above.

1.5 Identify the specific legal authorities, arrangements, and agreements that defined the collection of information.

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

The legal authority includes Title 20 Chapter IX Part 1001, and the authorization for operation of VBA PMCMS is VA Contract No. VA118-11-D-1000, and Title 38, United States Code, section 501(a) and Chapters 11, 13, 15, 18, 23,30, 31, 32, 34, 35, 36, 39, 51, 53, 55 VBAPMCMS SON995C/SOI VA08, Exhibit 300 # 029-00-01-22-01-1265-00, VBA Systems of Records Notice (SORN) # 58VA21/22/28.

1.6 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

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

<u>Principle of Purpose Specification:</u> The collection ties with the purpose of the underlying mission of the organization and its enabling authority.

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

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

Principle of Data Quality and Integrity: *VA policies and procedures must ensure that personally identifiable information is accurate, complete, and current.*
This is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk: PMCMS collects PII/PHI/SPI. Due to the sensitive nature of this data, there is a risk that if the data were accessed by an unauthorized individual or otherwise reached, serious harm may result for the individuals affected.

Mitigation: Electronic data is carried in a virtual private network (VPN) that utilizes industry standard technology and encryption algorithms (e.g., AES-256). VBA PMCMS CM Portal is rated as a Moderate impact system, in accordance with the Federal Information Processing Standards (FIPS)-199.All data elements processed and shared are specified by the VBA. As required by the contract, all data is treated as Sensitive (since it consists of a significant volume of PHI, PII, and SPI). Information is transmitted via the VBA's Business Partner Extranet (BPE).

Section 2. Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe how the information in the system that will be used in support of the program's business purpose.

Identify and list each use (both internal and external to VA) of the information collected or maintained. This question is related to privacy control AP-2, Purpose Specification.

PII/PHI Data Element	Internal Use	External Use
Name (First, Last, MI)	Veteran Identification purposes	Not used
Social Security Number	Veteran Identification purposes	Not used
Veteran File Number	Veteran Identification purposes	Not used
Integrated Control Number	Veteran Identification purposes	Not used
Zip Code	Benefits claim identification and routing	Not used
Email address	Veteran Identification purposes	Not used
VA File Number	Veteran Identification purposes	Not used
Service-Related Disabilities	Benefits claim identification and routing	

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

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

PMCMS CM Portal does not create new information. PMCMS CM Portal data are not analyzed outside of the scope defined by contract requirements.

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.

PMCMS CM Portal does not create new information. PMCMS CM Portal data are not analyzed outside of the scope defined by contract requirements.

2.3 How the information in the system is secured.
These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

2.3a What measures are in place to protect data in transit and at rest?

All data in transit and at rest are encrypted with FIPS 140-3 encryption algorithms.

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

There are no additional protections in place for SSNs in PMCMS CM Portal. SSNs are treated like all other PII that the system handles. We encrypt all metadata, including SSNs.

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

PMCMS CM Portal uses the FedRamp approved Amazon Web Services (AWS) Gov Cloud. Data is transmitted to VBMS via a dedicated S2S connection (CID 0555) with data uploaded via VBMS eFolder web service.

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?

PMCMS is governed by IAM policies (SSOi and SSOe) to manage accounts that enforces automated workflows for approval. PMCMS enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. PMCMS users are limited to the data needed to perform their specific job functions based on the user's role and location access granted. All users are required to complete annual initial and refresher privacy training, including Privacy Act, Health Insurance Portability and Account Ability Act (HIPPA), system/data security, and VA Rules of Behavior (ROB) training.

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

PMCMS CM Portal displays the system use notification on each screen of the system as well as a system use notification banner that defines authorized uses of the system prior to the user entering their login credentials, which defines the criteria, procedures, controls, and responsibilities regarding access. PMCMS also maintains SOPs for all Rev 5 security controls to which PMCMS is bound, including Access Control (AC), Personally Identifiable Information Processing and Transparency (PT), Incident Response (IR), and Awareness and Training (AT). All documentation is stored as artifacts in eMASS.

2.4c Does access require manager approval?

PMCMS CM Portal users require manager approval before being granted access to the system.

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

Yes. Every user or system that accesses the CM Portal is identified by a unique ID by which actions taken during their use of the system are recorded in audit and transaction logs, including viewing and / or modifying of any data associated with any document handled by the system.

2.4e Who is responsible for assuring safeguards for the PII as identified in eMASS?

It is the responsibility of each user of the PMCMS CM Portal to treat the information to which they have access with the appropriate security and privacy procedures including "need to know" in the performance of their job responsibilities. Leidos safeguards the information maintained within its systems in accordance with VA and DOD policy and security requirements.

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*

Information retained includes Name (First, Last, MI), SSN/VFN, zip code, email address, VA File Number, and Service-Related disabilities. Information is retained only to meet contractual business requirements.

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. If the system is using cloud technology, will it be following the NARA approved retention length and schedule https://www.archives.gov/records-mgmt/grs? This question is related to privacy control DM-2, Data Retention and Disposal.

PMCMS CM Portal retains packet and packet history data for the length of the contract, per the VA Business Requirements Document (BRD) specification. All PDF images are viewable in the PMCMS CM Portal for a minimum of one (1) year retention period following the data of the mail packet completion by the VA.

3.3 The retention schedule approved by the VA records office and the National Archives and Records Administration (NARA).

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

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

Yes, the system data retention schedule is specified and complies with the base contract, and any changes specified in the Interconnection Security Agreement (ISA)/Memorandum of Understanding (MOU). Information contained in the system is restricted to minimum required to meet system objectives.

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

PMCMS does not retain paper records. PMCMS CM Portal data is stored within the FedRamp Approved AWS Gov Cloud until end of contract, or as requested by our VA customer.

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.

At the conclusion of the PMCMS effort, all data is transitioned to the VA or their designated agent in accordance with our PWS Section 5.25.2. No data is retained in PMCMS after all data has been transitioned.

All data is stored in a Fed Ramp approved cloud storage service and is encrypted using FIPS 140-3 compliant encryption keys. Upon termination, PMCMS will follow best practices for the destruction of cloud storage objects and data whereby the cryptographic keys for all stored data and systems will be deleted, and the systems and stored objects/data also will be deleted.

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.

PMCMS does not determine nor control the use of PII for the purposes of research, testing, nor training. PMCMS only uses PII in accordance with our contract requirements to convert provided paper documents to e-documents. No data, PHI nor PII, is used outside of the

scope of the contracted requirements. PMCMS CM Portal does not use PII or PHI in any of its development or testing environments.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

Principle of Minimization: The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.

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

Follow the format below:

Privacy Risk: All data are kept until the end of the contract, per contract requirements; therefore, there is a risk of data being unintentionally released.

Mitigation: To mitigate the risk of release, the data is housed in a secure FedRamp approved AWS GovCloud database repository. Security controls are used to limit the access to this data; PMCMS authorizes access to privileged commands based on role (e.g., System Administrator, Applications Administrator, Database Administrator, Network Administrator, etc.). The assigned role can execute the privileged commands that are included in the rights profile for that role. Privileged access is restricted to PMCMS system administrators.

Users of the PMCMS CM Portal are assigned privileges and access according to their roles. All actions taken by users are audited and logged.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

PII Mapping of Components

4.1a **PMCMS** consists of 1 key component (servers/databases/instances/applications/software/application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **PMCMS** and the reasons for the collection of the PII are in the table below.

Note: Due to the PIA being a public facing document, please do not include server names in the table. The first table of 3.9a in the PTA should be used to answer this question.

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	**Does this system collect PII? (Yes/No)**	**Does this system store PII? (Yes/No)**	**Type of PII (SSN, DOB, etc.)**	**Reason for Collection/ Storage of PII**	**Safeguards**
DMHS CM Portal	Yes	Yes	Name (Last, First, MI) Social Security Number (SSN)/ Veteran File Number (VFN)/Integrated Control Number (ICN) Zip Code Email VA File Number Service-Related Disabilities	Transmit Veteran claim benefit information for claims processing	PIV or ID.me is required for access to the DMHS CM Portal. All non-public Portal access points are protected by deny-by-default whitelist firewalls Internal resources are hosted on protected private VPC subnets that are not publicly

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
					routable from the internet All data transmission and data-at-rest storage is encrypted. All public facing resources are monitored for malware, file integrity changes, and log monitoring.

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

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

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

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

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

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

Data Shared with Internal Organizations

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
VBMS	Transmit Veteran claim benefit information for claims processing	Name (Last, First, MI) Social Security Number (SSN)/ Veteran File Number (VFN)/Integrated Control Number (ICN) Zip Code Email VA File Number Service-Related Disabilities	Direct upload via eFolder API*. Currently, transmission is accomplished indirectly via the VA Claims Evidence API Adapter, which uses direct access to AWS S3 objects. *NOTE: This method of transmission has been deprecated and replaced by the VA Claims Evidence API Adapter. It is no longer used and will be decommissioned once approval is received from VBA.

4.2 <u>PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure</u>

Discuss the privacy risks associated with the sharing of information within the VA network and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions in this section.).

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

Follow the format below:

Privacy Risk: There is a risk that users of the PMCMS CM Portal System as a Service might disclose PII / PHI to coworkers who do not have a need to know the information.

Mitigation: Users of the PMCMS CM Portal are VA employees and contractors who are required to complete privacy and information security training annually. Systems and procedures are in place for identifying and reporting information security incidents.

Section 5. External Sharing/Receiving and Disclosure

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

5.1 List the external organizations (outside VA) that information shared/received. and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.

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

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

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

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

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

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

Data Shared with External Organizations

List IT System or External Program Office information is shared/received with	***List the purpose of information being shared / received / transmitted***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)***	***List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
N/A	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk: There is no external sharing. PMCMS will request authority to proceed PIV confirmation through SAML transmitted through the API. There is a slim risk that information may be shared with an external organization or agency.

Mitigation: There is no external sharing. Safeguards are implemented to ensure data is not shared with unauthorized organizations, including employee security and privacy training, and required reporting of suspicious activity. PIV cards are required to gain access. All measures that are utilized for the system, including ISA/MOU, which is reviewed at least annually to remain current and is monitored closely to ensure protection of information.

Section 6. Notice

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

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

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.

Notice is provided by VBA-Compensation, Pension, Education, and Vocational Rehab and Employment Records via the VBA Systems of Records Notice (SORN) # 58VA21/22/28 and this PIA. This is inherited from and handled by the VA. PMCMS only processes and stores data at the direction of VBMS, the data is not used for any other purpose.

6.1b If notice was not provided, explain why.

Notice is provided by VBA-Compensation, Pension, Education, and Vocational Rehab and Employment Records via the VBA Systems of Records Notice (SORN) # 58VA21/22/28 and this PIA.

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

Notice is provided by VBA-Compensation, Pension, Education, and Vocational Rehab and Employment Records via the VBA Systems of Records Notice (SORN) # 58VA21/22/28 and this PIA. This is inherited from and handled by the VA. PMCMS only processes and stores data at the direction of VBMS, the data is not used for any other purpose.

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.

Veterans have the right to refuse to disclose their SSNs to VBA. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VBA an SSN (please refer to the 38 Code of Federal Regulations CFR 1.575(a)).

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses, or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

All requests follow VA request channels, 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 VBA address outlined within the SORN 58VA21/22/28 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records. The administration of these requests is done by the VA and those requests are passed from the VA to PMCMS, not directly from any individuals to PMCMS. All information PMCMS receives comes directly at VA direction and it is up to VA to determine whether individuals can consent to particular uses of their information.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Follow the format below:

Privacy Risk: The individual may not be aware of published notice(s).

Mitigation: This PIA and the published SORN serves to notify Veterans about the collection, use, and storage of personal information. Notice, access, redress, and correction would be handled via the standard VA request channels for change. Their information is held in PMCMS only to provide enhanced access to VBMS, it is not used for any other purposes by PMCMS.

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 The procedures that allow individuals to gain access to their information.

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at VA Public Access Link-Home (efoia-host.com) to obtain information about FOIA points of contact and information about agency FOIA processes.***

It is outside of the scope of the PMCMS program to allow Veterans access to their information, as stored in the PMCMS CM Portal. This is inherited and handled by the VA. All requests MUST follow VA request channels. Veterans may request access to Privacy Act records maintained in PMCMS CM Portal by requesting a copy, in writing, via direct mail, fax, in person, or by mail referral from another agency or VA office to the VA directly.

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)?

All requests for information are outside of the scope of the PMCMS contract and are not administered by PMCMS. This is inherited and handled by the VA.

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?

It is outside of the scope of the PMCMS program to allow Veterans access to their information, as stored in the PMCMS CM Portal. This is inherited and handled by the VA. All requests MUST follow VA request channels. Veterans may request access to Privacy Act records maintained in PMCMS CM Portal by requesting a copy, in writing, via direct mail, fax, in person, or by mail referral from another agency or VA office to the VA directly.

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.

This is outside of the scope of the PMCMS program. This inherited and handled by the VA. However, Veterans have the right to amend their records by submitting their request in writing. 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 VBA Regional Office 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 VBA system of records, and the facility Privacy Officer or designee, and needs to be date stamped; and 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.

The procedure for correcting information is outlined above. Formal redress is provided. All information correction must be taken via the Amendment process. This is handled by the VA, it is outside the scope of this contract, and not administered by PMCMS.

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

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

Formal redress is provided. All information correction must be taken via the Amendment process. This is inherited from and handled by the VA, it is outside the scope of this contract for administration by PMCMS.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Principle of Individual Participation: *The mechanism by which an individual is able to prevent information about them obtained for one purpose from being used for other purposes without their knowledge.*
This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk: There is a risk that incorrect information is accidentally recorded in an individual's record.

Mitigation: PMCMS conversion vendors have controls and processes in place to ensure documents from one individual do not mistakenly get mixed into those from another individual; Those controls and processes are documented and maintained by conversion vendors and are outside of the scope of the PMCMS effort. PMCMS CM Portal does offer authorized users the capability to split packets so that if Veteran information is co-mingled, the authorized user may move the Veteran's information into the correct packet.

Section 8. Technical Access and Security

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

8.1 The procedures in place to determine which users may access the system, must be documented.
These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

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

New users register during their first sign on attempt for PMCMS CM Portal. The system retains user registration information for future access. The system checks account status and verifies the IAM authentication service used to access PMCMS CM Portal (SSOi/SSOe). The New Account Window displays, and the user is required to complete the information listed on the screen. The request is submitted automatically to the supervisor for the location(s) to which the user is requesting access. Upon supervisor approval, the user is notified via email that the account is approved.

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?

Users outside of VBA who require access to PMCMS CM Portal must have the VBA point of contact submit a new user request, via email to the PMCMS CM Portal team. Upon receipt of request, the PMCMS CM Portal team creates the user accounts and provides login access information to the users. Roles are determined by the VA, which determines the PII that can be shared.

8.1c Describe the different roles in general terms that have been created to provide access to the system? For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

PMCMS CM Portal has nine (9) standard VA user roles:

- Basic User – View assigned packets in work and hold queues; view all packets (not restricted) in search results, perform basic user functions on packets in search results, process packets in work queue and perform other tasks, including packet split, append document, add packet note, download packet documents, request rescan, upload packet to VBMS, etc.
- Basic User + Auto Assignment – Performs the same functions as a Basic User at assigned locations that participate in the Automatic Packet Assignment to the Work queue.
- Super User – Performs same functions as a Basic User at assigned locations, plus view all packet s for location assigned users in the work and hold queues; assign packet for processing to users at assigned locations that allow reassignment; process packets in the authorization queue; perform packet split on packets in the authorization and assignment queues; reassign packets in the reassign queue to a different location or line of business.
- Supervisor – Performs same functions as Super User at assigned locations plus process packets in the Unidentified Mail First Authorization queue.
- Supervisor + User Accounts – Performs same functions as the Supervisor plus approves/denies pending requests and manages Admin-User accounts at assigned locations.
- Records Management Officer – Process packets in Unidentified Mail Final Authorization queue, view packets, compare rescan documents in new packet with those in original packet, review packet and document history, download packet documents, view/add packet notes, mark packets as unread.
- National Reviewer – Read only access for packets in all locations, excluding those marked as restricted.
- Quality Assurance – Read only access for packets in all locations, including those marked as restricted.
- Contracting Officer Representative – Authorization to perform all functions on all packets at all locations, perform add/update/delete actions for user role/location/trigger document/emergent categories, send group emails, approve/deny pending requests for new, reactivated, and modified user accounts (only when COR has Account Request Approver secondary role).

8.2. Contractor signed Non-Disclosure Agreement (NDA), Business Associate Agreement (BAA) etc. in place.

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.

8.2a Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

> PMCMS CM Portal is a commercial System as a Service platform maintained for the purposes of the Veteran Benefits Administration. A VA security clearance is required for all persons having access to the systems or data, including PII. All CM Portal contractor staff are required to complete the appropriate VA annual training, including PISA/ROB training. ROBs are signed annually. The Performance Work Statement (PWS) establishes the privacy roles, responsibilities, and requirements for contractors having access to PII/PHI.

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

PMCMS CM Portal is a commercial System as a Service platform maintained for the purposes of the Veteran Benefits Administration. The PMCMS staff (VA contractors) develop the application and have access to the system and the associated PII housed within the database. A VA security clearance is required for all persons having access to the systems or data, including PII. All CM Portal contractor staff are required to complete the appropriate VA annual training, including PISA/ROB training. ROBs are signed annually. The Performance Work Statement (PWS) establishes the privacy roles, responsibilities, and requirements for contractors having access to PII/PHI.

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

PMCMS CM Portal is a commercial System as a Service platform maintained for the purposes of the Veteran Benefits Administration. The PMCMS staff (VA contractors) develop the and maintain the application.

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.

All persons associated with PMCMS CM Portal development, operation, and maintenance receive initial entry, annual refresher, and ad hoc training on privacy, including the Privacy Act, HIPAA, system and data security, and the VA Rules of Behavior. Additional VA training, including role-based training is required for personnel with specific roles (developer, program manager, database administration, and system administration).

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

Authorization to Operate (ATO) PMCMS, A FIPS Publication 199 Moderate system, was last granted on 30 April 2025 for 1 year.

8.4a If completed, provide:

1. *The Security Plan Status:* not approved yet
2. *The System Security Plan Status Date:* 30 April 2025
3. *The Authorization Status:* Authority to Operate
4. *The Authorization Date:* 30 April 2025
5. *The Authorization Termination Date:* 30 April 2026
6. *The Risk Review Completion Date:* 30 April 2025
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

8.4b If not completed or In Process, provide your ***Initial Operating Capability (IOC) date.***

N/A

Section 9 – Technology Usage

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

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

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

PMCMS CM Portal uses the FedRamp Approved AWS GovCloud.

9.2 Does the contract with the Hosting Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). ***(Refer to question 3.3.1***

of the PTA) *This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

AWS policy is that the customer accounts own and maintain sole control of all data in the service account (https://aws.amazon.com/compliance/data-privacy/). PMCMS CM Portal owns and manages the system; the VA owns the data.

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

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

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

AWS collects ancillary data for the purposes of auditing activities and billing for service usage. Presumably AWS owns this data to use for its business purposes.

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

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met?

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

Per AWS documentation, the customers own and are responsible for controlling and securing the data stored in the cloud account. (Source: https://aws.amazon.com/compliance/data-privacy-faq/)

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

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

The PMCMS CM Portal does not utilize RPA for any of its operations. Other VA programs and contracts utilize RPA to access and process data and documents in the CM Portal. All access and actions taken on data and documents in the CM Portal are tracked, audited, and linked to the identity of the entity (human and / or automaton) that executed those actions.

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**

ID	Privacy Controls
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.

MARVIS HARVEY

Digitally signed by MARVIS HARVEY
Date: 2025.06.30 10:38:12 -05'00'

Privacy Officer, Marvis Harvey

ROGER CARROLL

Digitally signed by ROGER CARROLL
Date: 2025.06.30 12:03:58 -04'00'

Information System Security Officer, Roger Carroll

JOHN CLARK

Digitally signed by JOHN CLARK
Date: 2025.07.02 11:23:31 -05'00'

Information System Owner, John Clark

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy; a Privacy Act notice on forms; screen shot of a website collection privacy notice).

Notice is provided by VBA-Compensation, Pension, Education, and Vocational Rehab and Employment Records via the VBA Systems of Records Notice (SORN) # 58VA21/22/28 and this PIA. This is inherited from and handled by the VA. PMCMS only processes and stores data at the direction of VBMS, the data is not used for any other purpose.

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

VA Privacy Service Privacy Hub:
https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):
VHA Directive 1605.04
IB 10-163p (va.gov)