Privacy Impact Assessment for the VA IT System called:

Veterans Benefits Management System (VBMS) Cloud Assessing

OIT Benefits, Appeals and Memorials Portfolio
Veterans Benefits Administration

Date PIA submitted for review:

3/1/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Tonya Facemire	Tonya.facemire@va.gov	202-632-8423
Information System Security Officer (ISSO)	Joseph Guillory	Joseph.guillory@va.gov	619-204-6840

	Name	E-mail	Phone Number
Information System Owner	Gary Dameron	Gary.dameron2@va.gov	202-492-1441

Abstract

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

Veterans Benefits Management System (VBMS) Cloud Assessing is an integrated web application intended to streamline Veteran's disability claims process by providing claims processors with an electronic, paperless environment in which to maintain, review, and make rating decisions for veterans' claims. VBMS is a system of systems that interconnects with many local and disparate software components. VBMS can be decomposed into systems of interconnectivity, layers within each information system, and software components that comprise and integrate these layers. The application is hosted in a cloud-based environment utilizing Virtual servers to deliver Veteran's information and evidence for processing via a web browser. End-to-end claims processing provides functionality required for establishment, development, rating, award, and appeal of a claim. It is the intent of this effort to deliver VBMS incrementally using an agile development methodology based upon the priorities determined by Office of Information Technology (OIT).

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.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *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? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

VBMS is a System of Record, as noted by the 2012 58VA21/22/28 SORN located at 2021-24372.pdf (govinfo.gov).
Veterans Benefits Management System (VBMS) is a multi-year technology solutions project to transition Veterans Benefits Administration (VBA) from a paper-intensive claims processing environment to a paperless-based environment. The goal of this program is to provide VBA with systems engineering support for the overall design of the VBMS solution (to include security components). This support also includes test and integration services and the development of VBMS, the development of Service Oriented Architecture (SOA) objects, the development of services for the user interface to communicate with the corporate database, the development of the VBMS database, security to meet the requirements of VA Directive 6500 Information Security Handbook, and the development of functionality to support end-to-end claims processing in an electronic environment. End-to-end claims processing provides functionality required for establishment, development, rating, award, and appeal of a claim. It is the intent of this effort to deliver VBMS incrementally using an agile development methodology based upon the priorities determined by Office of Information Technology (OIT). VBMS is a system of systems that interconnects with many local and disparate software components. VBMS can be decomposed into systems of interconnectivity, layers within each information system, and software components that comprise and integrate these layers.

VA Enterprise Cloud Solutions group partnered with Amazon Web Services (AWS) a FedRAMP provider to offer VA programs the opportunity to host cloud applications. VBMS production environment is hosted in AWS under VA Enterprise Cloud Solutions Office (ECSO) General Support System (GSS) and accredited as FISMA "HIGH" categorization. Custody and ownership of PII and PHI are solely the responsibility of the VA as a tenant of AWS, in accordance with VA policy and NIST 800- 144. Both AWS and the VA have a tremendous interest in maintaining security of PII and PHI, including (but not limited to) HIPAA Enforcement Rule of 2006, HIPAA Omnibus, and HITECH. AWS is responsible for physical security, infrastructure security, network and communications for the facility. VA is responsible for the maintaining application, data and system security for the program. VA is the sole owner of all data stored within the system.

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. SSN serves as the Medical Record Number and Unique Identifier for the Veteran in this and all VA OI&T Systems. Executive Order 9397, which allows the collection and use for business purposes/enrollment and 32 CFR 505.4(a)(b) for individual's rights, benefits, and privileges under federal programs serves as the highest legal authority for this use.

VBMS is designed, built, operated, and maintaining with the requirement to contain records that have Veterans PII and PHI (which number in tens of millions). As such, the completion of this PIA will not result in any circumstances that could potentially require changes to business practices nor result in technology changes.

VBMS does not communicate with any external entities outside of VA purview, but ingests a variety of information internal to the Department of Veteran's Affairs. VBMS conducts a variety of information sharing internal to the Department of Veterans Affairs. Internal sharing discussed in greater detail in Section 4 of this Privacy Impact Assessment (PIA).

VBMS collects Personally Identifiable Information (PII) and other highly delicate Personal Health Information (PHI). If this information was breached or accidentally released to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to the individuals whose information is contained in the system.

Section 1. Characterization of the Information

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

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

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

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

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

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

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☒ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☒ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☒ Financial 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
- ☒ Gender
- ☐ Integration Control Number (ICN)
- ☒ Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Unique Identifying Information (list below)

Additional Information Collected But Not Listed Above: Maiden Name, Alias, Driver's License Number, Family Relation, Guardian Information, Benefit Information

PII Mapping of Components

Veterans Benefits Management System (VBMS) Cloud Assessing consists of **four** key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **Veterans Benefits Management System (VBMS) Cloud Assessing** and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

Note: Due to the PIA being a public facing document, please do not include the server names in the table.

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Database names are not identified in the VBMS application interconnection. Receiving systems manage internal information delivery as part of their receiving application	Yes	Yes	Social Security Number, DOB, Medical Records, Disability and Compensation	Veteran data required to process claims and pay benefits	VA Network only which requires VPN access and 2 Factor Authentication thru the Trusted Internet Connection (TIC) Gateway

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.

VBMS system receives information directly from the application's user interface (UI) and electronically, via web services. VBMS receives information from Benefit Gateway Services (BGS), Common Security Services (CSS), Virtual VA (VVA), Master Veteran's Index (MVI), Clinical User Interface (CUI), Digits to Digits (D2D), Enterprise Veteran Self Service (EVSS), VONAPP Direct connect (VDC), Stakeholder Enterprise Portal (SEP), eBenefits, and Customer Relationship Management (CRM), Solutions Made Simple (SMS), and CSRA.

Scanning vendors are under the Veteran's Claims Intake Programs (VCIP), which currently has two contractors, SMS and CSR. VCIP is used to scan-in paper documents that exist for veterans that were used during the legacy paper claim filing process. Scanning vendors are not considered external connections by VA definition because traffic is in-bound only through a bulk device VPN TIC gateway. The VBMS user interface assists with veteran claim data (filed by Veteran Service Organization (VSO), veterans, or other sources), veteran exam results, and additional evidence in relations to filed claims.

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.

Information is collected from VBA claims processers in the Region Offices (RO) as input through the web UI. Scanning vendors, SMS and CSRA, scan in paper documents that exist for veterans, remotely via web services into the VBMS document repository. VBMS receives claims information electronically, via web services from VA hospitals and health care providers.

1.4 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.

As information is imported from VA healthcare providers, the accuracy is verified by the original source. Veteran information that is retrieved from CORPDB is validated via BGS and veteran information queried through the UI is validated via MVI. Prior to any award or entitlement authorization(s) by the VBMS, the veteran record is manually reviewed, and data validated by the Veteran Service Representative (VSR) and the Rating Veteran Service Representative (RVSR) to ensure correct entitlement has been approved.

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

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

The VA employee's BDN, VETSNET or VBMS identification numbers, the number and kind of actions generated and/or finalized by each such employee, the compilation of cases returned for each employee falls under the authority of the following: 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. SSN serves as the Medical Record Number and Unique Identifier for the Veteran. The legal authority is Executive Order 9397, which allows the collection and use of SSN for business purposes/enrollment and 32 CFR 505.4(a)(b) for individual's rights, benefits, and privileges under federal programs. VBMS is a System of Record, as noted by the 2012 58VA21/22/28 SORN located at 2021-24372.pdf (govinfo.gov).

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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: VBMS collects Personally Identifiable Information (PII) and other highly delicate Personal Health Information (PHI). This information is specifically collected for the purpose of VBMS as a system. It is an absolute requirement for the efficacy of VBMS.
If this information was breached or accidentally released to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to the individuals whose information is contained in the system.

Mitigation: The Department of Veterans Affairs is careful to only collect the information necessary to identify the parties involved in an incident, identify potential issues and concerns, and aid the affected parties so that they may find the help they need to get through their crisis. By only collecting the minimum necessary information specified in section 1.1, the VA can better protect the individual's information. VBMS is built on the existing VBA Common Security System (CSS) that controls user authentication and role-based permissions. Permissions are only given after a request and approval of that request by an Information Security Officer (ISO).
Because of the nature of VBMS, information is collected from health care providers, VBA claims, and scanning vendors. Individuals do not have the authority to opt into the VBMS participation but can opt out through a developed and mature process. The amount of information collected is the minimum amount required to make such decisions.
VBMS provides additional security to VBA CSS for both integrity and confidentiality which will prevent unauthorized users from gaining access to any data. Additionally, VBMS is an internally hosted application meaning that only the authorized user can access VBMS and those users have to be on the VA network which insulates VBMS from any outside/public access. VBMS employ a variety of security measures that satisfy controls dictated within the VA 6500 Rev 4 Directive.

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.

Full Name: Veteran Identification
DOB: Used to verify Veteran's identity
Maiden Name: Used to verify Veteran's identity
Mother's Maiden Name: Used to verify Veteran's identity
Alias: Used to verify Veteran's identity and also as reference
SSN: Used to verify Veteran's identity and as a file number for Veteran
Veteran Driver's License: Used to verify Veteran's identity
Race / Ethnicity: Used to verify Veteran's identity
Taxpayer Identification Number: Used as a file number for Veteran
Financial Account Number: Used as a reference for the Veteran's account
Mailing Address: Used to correspond with the Veteran
Phone Number: Used to correspond with the Veteran
Family Relation: Used for Veteran's family benefits
Military Service Information: Used to determine benefits eligibility
Medical Information: Used to track medical information
Guardian Information: Used to verify if Veteran's family member has guardian
Benefit Information: Used to determine benefit eligibility
Personal Email Address: Used to correspond with the Veteran
Current Medications: Used to track medication history

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

VBMS uses Scorecard to provide VBA with active claims statistics for a given regional office. This produces data that will be used to determine rulesets for National Work Queue (NWQ) to route claims to other regional offices. VBMS uses advanced analytics to suggest body systems to users of VBMS-R based on large historic claim data sets. This produces the suggested body system code for raters to use for the appeals and awards process.

2.3 How is the information in the system secured?

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

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

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

This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest

All sensitive and confidential data is encrypted using FIPS 140-2 compliant AES-256 encryption algorithms in transit and at rest. The information includes objects in VAEC AWS GovCloud s3 buckets, EBS volumes, and databases. AWS uses EBS encryption (AES-256 algorithms) which uses AWS Key Management Service keys when creating encrypted volumes and snapshots.

VBMS inherits some of the implementation of this control from VA OIT and AWS GovCloud High accreditation package. Documents are transmitted to VBMS through electronic system interfaces and the VBMS WebUI document upload feature. All interfaces for uploading documents are protected by A& A controls at the network and application layers. VBMS components guarantee the confidentiality and integrity of data transmissions between VBMS and other parties with IP security between the communicating nodes at the transport layer. VBMS uses NFS for file sharing within database clusters.

2.4 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.

VBMS is a System of Record, as noted by the 2012 58VA21/22/28 SORN located at 2021-24372.pdf (govinfo.gov) defines the information collected from Veterans, use of the information, and how the information is accessed and stored. The information collected is to support the individual claim or claims the veteran has been granted. The security controls for the VBM application cover 26 security areas regarding 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; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; program management; planning; personnel security; risk assessment; systems and services acquisition; security assessment and authorization; system and communications protection; system and information integrity; authority and purpose; accountability, audit, and risk management; data quality and integrity; data minimization and retention; individual participation and redress; security; transparency; use limitation. The VBM application team has implemented the required security controls based on the tailoring guidance of NIST Special Publication 800-53 Rev 4 and VA directives or handbooks. VA Records Management Policy VA 6300.1, VA 6500 HB, National Rules of Behavior (ROB), and VA 6502.1, VA6502.3, 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

Full Name, Maiden Name, Mother's Maiden, Name Alias, Social Security Number, DOB, Driver's License Number, Taxpayer Identification Number, Financial Account Number, Mailing Address, Zip Code, Phone Numbers, Email Address, Family Relation, Service Information, Medical symptoms, Diagnoses, Medical Information, Guardian Information, Benefit Information, Current Medications, Previous Medical Records, Race

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?

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.

All the data will be retained for five years. All VA and VAMC provided information is destroyed at the end of the contract.

Recovery Audit System Files: Inputs- destroy/delete source data after data is entered into the master file or database and verified, or when no longer needed to support construction of, or serve as backup to, the master file or database, whichever is later.

Prior to decommissioning of system(s), AWS must receive written approval from the VA before any VA provided information is destroyed. Any data destruction done on behalf of the VA must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in GRS 3.1 and GRS 3.2 (GRS 20).

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.

These records are retained and disposed of in accordance with the General Records Schedule 3.1 and 3.2 (GRS 20), approved by National Archives and Records Administration (NARA)
https://www.archives.gov/records-mgmt/grs.html

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

Records/digital information will be eliminated following the sanitization procedures in VA Handbook 6300.1
Records Management Procedures and VA Handbook 6500.1 Electronic Media Sanitization.

All remaining paper records (after scanning) are shredded using an approved National Security Agency (NSA) High Security Crosscut Shredder from the NSA High Security Crosscut Shredder List.

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

VBMS does not use any PII or PHI in the test, prod-test, or pre-production environments, thus minimizing the risk of exposing PII. The IA team has automated scripts that run in these environments to test for the leakage of actual PII into an environment not authorized as such.

3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.

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:

<u>Principle of Minimization:</u> 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 by VBM 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: To mitigate the risk posed by information retention, VBM adheres to the NARA General Records Schedule. When the retention date is reached for a record, the individual's information is carefully disposed of by the determined method as described in General Records Schedule 20.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Benefit Gateway Service (BGS)	BGS is the gateway into the Corp DB which was previously the authoritative source for most of the veteran and claim data for VBA	Detailed data elements are too many to list and would be virtually everything to do with a veteran, veteran demographics, veteran claims, claims adjudication, and claim award.	SOAP over HTTPS using SSL encryption and Certificate Exchange
Data Access Services (DAS)	DAS is the common service that exchanges information with other agencies both within VA and external to VA	- Name - SSN - DOB - Mother's Maiden Name - Personal Mailing Address - Personal Email Address - Financial Account Information - Current medications - Race / Ethnicity - Tax Identification Number - Gender - Military History / Service Connection	SOAP over HTTPS using SSL encryption and Certificate Exchange
Performance Analysis & Integrity (PA&I)	PA&I uses a daily extract of claim and work item data to produce reports and metrics for VBMS	- System Log Files - SSN - DOB - Mother's Maiden Name - Personal Mailing Address - Personal Email Address - Financial Account Information - Current Medications - Race / Ethnicity	SFTP

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		- Tax Identification Number - Gender - Military History / Service Connection	
VONAPP Direct Connect (VDC) and the Stakeholder Enterprise Portal (SEP)	Veterans Online Application (VONAPP) Direct Connect (VDP) and the Stakeholder Enterprise Portal (SEP) allow claimants to file disability compensation and dependency applications directly to SOO via eBenefits. VBMS is the document repository for claims materials submitted through VDC.	- Name - SSN - DOB - Mother's Maiden Name - Personal Mailing Address - Personal Email Address - Financial Account Information - Current Medications - Race / Ethnicity - Tax Identification Number - Gender - Military History / Service Connection	VDP connects through DAS using SOAP over SSL. This is encrypted traffic secured by Certificate Exchange.
Virtual VA (VVA)	VVA is the electronic storage for applications and evidence, plus all correspondence and ratings sent out from the Department of Veteran Affairs.	- Name - SSN - DOB - Mother's Maiden Name - Personal Mailing Address - Personal Email Address - Financial Account Information - Current Medications - Race / Ethnicity - Tax Identification Number - Gender - Military History / Service Connection.	VVA connects through DAS using SOAP over SSL. This is encrypted traffic secured by Certificate Exchange.

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
Clinical User Interface (CUI)	CUI provides exam responses unidirectionally to VBMS Core to populate Ratings, Correspondence, and Awards data	- Name - SSN - DOB - Mother's Maiden Name - Personal Mailing Address - Personal Email Address - Financial Account Information - Current Medications - Race / Ethnicity - Tax Identification Number - Gender - Military History / Service Connection	CUI connects unidirectionally through DAS using SOAP over SSL. This is encrypted traffic secured by Certificate Exchange.
Enterprise Veteran Self-Service (EVSS) and eBenefits	EVSS and eBenefits both allow Veterans to initiate and submit a claim establishment on their own behalf through VMBS to BGS.	- Name - SSN - DOB - Mother's Maiden Name - Personal Mailing Address - Personal Email Address - Financial Account Information - Current Medications - Race / Ethnicity - Tax Identification Number - Gender - Military History / Service Connection	EVSS / eBenefit connects through DAS using SOAP over SSL. This is encrypted traffic secured by Certificate Exchange.
Digits to Digits (D2D)	D2D is a data delivery service built to enable the VSOs to electronically submit data and	- Name - SSN - DOB - Mother's Maiden Name	D2D connects through DAS using SOAP over SSL. This is encrypted traffic secured by

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
	related attachments from its CMS to VA systems using a standardized and centralized method.	- Personal Mailing Address - Personal Email Address - Financial Account Information - Current Medications - Race / Ethnicity - Tax Identification Number - Gender - Military History / Service Connection.	Certificate Exchange.
Scanning Vendors: Solutions Made Simple (SMS) and CSRA	Scanning vendors turn literal tons of paper files into scanned images of paper documents and attach them as evidence to Veteran's ID and claim numbers.	- Name - SSN - DOB - Mother's Maiden Name - Personal Mailing Address - Personal Email Address - Financial Account Information - Current Medications - Race / Ethnicity - Tax Identification Number - Gender - Military History / Service Connection	Documents are uploaded through DAS using SOAP over SSL. This is encrypted traffic secured by Certificate Exchange, and are only referenced by metadata.
Veterans Benefits Administration (VBA)	Information is shared across VBA to facilitate Veterans benefits claim processing.	Detailed data elements are too many to list and would be virtually everything to do with a veteran, veteran demographics, veteran claims, claims adjudication, and claim award.	Compensation and Pension Record Interchange (CAPRI) electronic software package.

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 PII is that sharing data within the Department of Veterans' Affairs could happen and the data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

Mitigation: The potential harm is mitigated by access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance, accountability, audit and risk management, data quality and integrity, data minimization and retention, individual participation and redress, need-to-know, transparency and use limitation.

Electronic Permission Access System (ePAS) mitigates the risk of inadvertently sharing or disclosing information by assigning access permissions based on need to know. Only personnel with a clear business purpose for accessing the information are allowed to access VBMS and the information contained within.

The use of a Personal Identity Verification (PIV) card is implemented. This ensures the identity of the user by requiring two-factor authentication

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
N/A				

VBMS 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 VBMS 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** VBMS 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.

The Department of Veterans Affairs does provide public notice that the system does exist. When Veterans apply for benefits, The Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected information to individuals applying for benefits. A signed statement acknowledging that they individual read and understood the NOPP is scanned into each applicant's electronic file. When updates are made to the NOPP copies are mailed to all Veteran's beneficiaries. Additionally, new NOPPs are mailed to beneficiaries on a yearly basis and periodic monitoring is performed to check that the signed acknowledgment form has been scanned into electronic records.

Additional notice is provided through this Privacy Impact Assessment, which is available online, as required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs and the following VA System of Record Notices (SORNs) which are published in the Federal Register and available online: The System of record Notice (SORN) "Compensation, Pension, Education, and Rehabilitation Records-VA" 58VA21/22/28 dated 11/8/2021. The SORN can be found online at 2021-24372.pdf (govinfo.gov).

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 and Service members may not decline or request that their information not be included as part to determine eligibility and entitlement for benefits. No penalty or denial of service is attached with not providing needed information; however, services may be delayed.

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

While individuals may have the ability to consent to various uses of their information at the VA, they are not required to consent to the use of their information as part to determine eligibility and entitlement for benefits.

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 VBM 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 in question 6.1, including the Privacy Impact Assessment and the System of Record Notice.

Section 7. Access, Redress, and Correction

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

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

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 VBMS. An individual who wishes to determine whether a record is being maintained under his or her name in VBMS 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 in VBMS 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 ensures 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. VBMS 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.

Follow the format below:

Privacy Risk: There is a risk that individuals may seek to access or redress records about them held by the VA Office and become frustrated with the results of their attempt.

Mitigation: By publishing this PIA, and the applicable SORN, the VA makes the public aware of the unique status of applications and evidence files, such as those stored on the Virtual VA platform. Furthermore, this document and the SORN provide the point of contact for members of the public who have questions or concerns about applications and evidence files.

Section 8. Technical Access and Security

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

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

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.

Access to VBMS is controlled through form authentication and assigned user roles, each with unique combinations of privileges within the system. All users of the VBMS are required to complete annual information system security training activities including security awareness training and specific information system security training. Annual training on VA Privacy and Information Security Awareness is tracked on the VA TMS. All users of the VBMS are required to complete annual information system security training activities including basic security awareness training and specific information system security training provided via the Talent Management System (TMS).

Access to VBMS working and storage areas is restricted to VA employees and authorized Contractors who must complete both the HIPAA and Information Security training using TMS. Specified access is granted based on the employee's functional category. Role based training is required for individuals with significant information security responsibilities to include but not limited to Information Security Officer (ISO), local Chief Information Officer (CIO), System Administrators, Network Administrators, Database Managers, Users of VA Information Systems or VA Sensitive Information.

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.

Access to computer rooms at the AWS facility is limited by appropriate locking devices and restricted to authorized VA employees and vendor personnel. Automated Data Processing (ADP) peripheral devices are placed in secure areas (areas that are locked or have limited access) or are otherwise protected. VA furnished laptops and similar devices are protected with two-factor authentication and OS level encryption at rest.

Access to information stored on automated storage media at other VA locations is controlled by individually unique passwords/codes. Access by Office of Inspector General (OIG) staff conducting an audit, investigation, or inspection at AWS facility is supervised and rigorously controlled.

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

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

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

Yes, the VBMS 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 Security Plan Status,*
2. *The Security Plan Status Date,*
3. *The Authorization Status,*
4. *The Authorization Date,*
5. *The Authorization Termination Date,*
6. *The Risk Review Completion Date,*
7. *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.***

System Security Plan Status: Approved
System Security Plan Status Date: Aug 12, 2021
System Authorization Status: Approved
System Authorization Date: Aug 12, 2021
System Authorization Termination Date: Aug 12, 2022
System Risk Review Completion Date: March 15, 2022
FIPS 199 Classification of System: HIGH

Section 9 – Technology Usage

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

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

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

This question is related to privacy control UL-1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1.

VBMS utilizes the VA Enterprise Cloud (VAEC) as it's cloud service provider.

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

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

VBMS utilizes the VA Enterprise Cloud (VAEC) as it's cloud service provider.

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.

VBMS utilizes the VA Enterprise Cloud (VAEC) as it's cloud service provider.

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.

VBMS utilizes the VA Enterprise Cloud (VAEC) as it's cloud service provider.

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

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the

automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).

N/A

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

ID	Privacy Controls
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.

Tonya L. Facemire 234776

Digitally signed by Tonya L. Facemire 234776
Date: 2022.04.05 20:01:18 -04'00'

Privacy Officer, Tonya Facemire

Joseph A. Guillory 1085540

Digitally signed by Joseph A. Guillory 1085540
Date: 2022.04.05 14:10:15 -07'00'

Information System Security Officer, Joseph Guillory

Gary W. Dameron 101941

Digitally signed by Gary W. Dameron 101941
Date: 2022.04.05 04:43:03 -04'00'

Information System Owner, Gary Dameron

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).

Notice of Privacy Practices

This system is intended to be used by authorized VA network users for viewing and retrieving information only except as otherwise explicitly authorized. VA information resides on and transmits through computer systems and networks funded by VA; all use is considered to be understanding and acceptance that there is no reasonable expectation of privacy for any data or transmissions on Government Intranet or Extranet (non-public) networks or systems. All transactions that occur on this system and all data transmitted through this system are subject to review and action including (but not limited to) monitoring, recording, retrieving, copying, auditing, inspecting, investigating, restricting access, blocking, tracking, disclosing to authorized personnel, or any other authorized actions by all authorized VA and law enforcement personnel. All use of this system constitutes understanding and unconditional acceptance of these terms. Unauthorized attempts or acts to either (1) access, upload, change, or delete information on this system, (2) modify this system, (3) deny access to this system, or (4) accrue resources for unauthorized use on this system are strictly prohibited. Such attempts or acts are subject to action that may result in criminal, civil, or administrative penalties.

PRIVACY ACT INFORMATION: The VA will not disclose information collected on this form to any source other than what has been authorized under the Privacy Act of 1974 or Title 38, Code of Federal Regulations 1.576 for routine uses (i.e., civil or criminal law enforcement, congressional communications, epidemiological or research studies, the collection of money owed to the United States, litigation in which the United States is a party or has an interest, the administration of VA Programs and delivery of VA benefits, verification of identity and status, and personnel administration) as identified in the VA system of records, 58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA, published in the Federal Register. Your obligation to respond is required to obtain or retain benefits. VA uses your SSN to identify your claim file. Providing your SSN will help ensure that your records are properly associated with your claim file. Giving us, your SSN account information is voluntary. Refusal to provide your SSN by itself will not result in the denial of benefits. The VA will not deny an individual benefit for refusing to provide his or her SSN unless the disclosure of the SSN is required by Federal Statute of law in effect prior to January 1, 1975, and still in effect. The requested information is considered relevant and necessary to determine maximum benefits under the law. The responses you submit are considered confidential (38 U.S.C. 5701). Information submitted is subject to verification through computer matching programs with other agencies