Privacy Impact Assessment for the VA IT System called:

Integrated Benefits System (IBS)

Veterans Benefits Administration (VBA)

Benefits, Appeals, and Memorials (BAM)

Date PIA submitted for review:

05/11/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Jean-Claude Wicks	Jean-Claude.Wicks@va.gov	202-502-0084
Information System Security Officer (ISSO)	Joseph Facciolli	Joseph.Facciolli@va.gov	212-842-2999x2012
Information System Owner	Christina Lawyer	Christina.lawyer@va.gov	518-210-0581

Abstract

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

The Integrated Benefits Services (IBS) system provides authorized applications access to data that was historically stored in Beneficiary Identity Record Locator Subsystem (BIRLS) but have since been migrated to other VA databases. The data presented through IBS provides VA customers with verified Veteran data used to process claims and verify military service.

Overview

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

1 General Description

A. The IT system name and the name of the program office that owns the IT system.

Integrated Benefits System (IBS) helps to fulfill the Veterans Benefits Administration (VBA) BAM Program office's prioritized objective to minimize redundancies within the VA Enterprise Architecture by allowing the decommissioning of the legacy BIRLS mainframe database. Once historical BIRLS data is migrated to other VA databases, IBS allows VA customers to access the historical BIRLS data from its new location without interruption.

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

IBS is a minor application responsible for allowing VA customers to access historical BIRLS data from its new location.

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

Office of Information Technology (OIT)

2. Information Collection and Sharing

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

Data includes over 48 million veteran records dating back to the Civil War. A typical client includes Veterans attempting to process claims and verify military service.

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

The system controls the assignment of file numbers, inactive compensation, and pension data, and both active and inactive insurance policy numbers. The purpose of this information is for consumers such as VA National Call Center (NCC) Specialists, Insurance Center Specialists, and Claims Examiners to process Veteran/Beneficiary inquiries.

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

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

IBS services, built within BIP, leverage the FEDRAMP-approved VA Enterprise Cloud (VAEC) Amazon Web Services (AWS) GovCloud environment, deployed in a single instance across three Availability Zones. PII is stored in encrypted databases. Security and privacy data held by a cloud provider is still required to meet the requirements under the privacy act. Federal agencies are required to identify and assess the risk to their PII, and to ensure security controls are implemented to provide adequate safeguards. Section C MM. of the contract references OMB Memorandum "Security Authorization of Information Systems in Cloud Computing Environments" FedRAMP Policy Memorandum.

3. Legal Authority and SORN

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

58VA21 - Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA
45VA21 – Veterans Assistance Discharge System-VA
138VA0005Q - Veterans Affairs Department of Defense Identity Repository (VADIR) - VA

I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?

The SORN will not require amendment or revision. The current SORN covers cloud usage and storage.

D. System Changes

J. Whether the completion of this PIA will result in circumstances that require changes to business processes
Completion of this PIA is not expected to result in a change to business processes.

K. Whether the completion of this PIA could potentially result in technology changes
Completion of this PIA is not expected to result in a change of technology processes.

Section 1. Characterization of the Information

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

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

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

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

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

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

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☒ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☐ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☐ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers*
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☐ Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☐ Gender
- ☐ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Data Elements (list below)

The SPI transmitted through IBS includes the items checked above as well as the following:
- Service Number
- Active service amount
- Branch of service
- Character of service
- Pay grade
- Assigned separation reason
- Service period
- Service-connected disabilities & diagnostics
- Reenlisted indication
- Purple Heart or other military decoration indication
- Date of death

• File Number
• Enlistment Date

PII Mapping of Components (Servers/Database)

IBS consists of **one** key components (servers/database). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **IBS** and the reasons for the collection of the PII are in the table below.

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

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
CorpDB	Yes	Yes	Name File Number Social Security Number Birthdate	Confirmation and verification of Veterans Identify.	RLS application team verifies that DB is up to date with versioning security standards.

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

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

-Veterans Assistance Discharge Systems (VADS)
-Veterans Benefits System (VBA) Applications:
- Benefits Delivery Network (BDN) – provides Compensation & Pension, Education, and Vocational Rehabilitation and Employment (VRE) information
- Corporate Database (CorpDB) – provides service and identity information
- Insurance Payment System (INS) – provides Veteran Insurance information
- Master Person Index (MPI) – provides Veteran/Beneficiary identify information
- Veterans Benefits Management System (VBMS) – provides Veteran/Beneficiary information
- VBMS Core – provides Veteran information from VBMS to ICP API for processing
- VA/DoD Identity Repository (VADIR) – provides eligibility and benefits utilization data across VA and DoD

- Tuxedo Proxy – provides Veteran/Beneficiary information from Share application to Folder Location API

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.

VADS supplies Veteran DD-214 information used to identify the Veteran and determine benefits. VBA apps provide additional data points necessary for processing Veteran inquiries.

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

N/A

1.3 How is the information collected?

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

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

Yes

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

Regularly scheduled batch jobs (daily, monthly, etc.) from some of the sources listed in Section 1.3 send data updates through IBS to the appropriate authoritative source. Specifically, INS produces monthly batch files that IBS processes and uses to update Veteran Insurance data. In addition, VADIR and VADS regularly feed military service data to other VA applications through IBS. VBMS sends batch files to the Pentaho server for data storage on the AWS RDS DBs.
Besides automated data collection and synchronization, NCC agents, Insurance Center Specialists, and Claims Examiners at VA Regional Offices (ROs) work with Veterans/Beneficiaries to retrieve information and process benefits inquiries. Although these RO specialists do not log in to IBS directly, they can update data within VA sources through IBS by using an interface provided by another application.

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

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

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is

there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

1.4b If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

Data quality is verified by use of the existing cloud technology infrastructure. AWS RDS security is utilized for the storage of data within the Folder Location and RDS Staging databases. Secure transmission of data is ensured through use of the existing VA network using prescribed protocols. Data accuracy is maintained by use of existing data integrity measures already included in the VA system. Data processing integrity is maintained through use of the ETL software.
VA staff review DD-214 forms before entering Veteran information into VADS to upload via IBS on a nightly basis. Additionally, authorized VA staff can update data directly through IBS using one of the applications listed in Section 1.2. Any user interfaces for entering Veteran information ensures the data entry is correct by disallowing invalid characters and formats. Furthermore, upon receiving new information from the batch jobs described in Section 1.3, IBS confirms that each data element is valid before passing data updates to the receiving database.

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

Title 10 U.S.C. Chapters 106a, 510,1606 and 1607; and Title 38, U.S.C. Section 501(a) and Chapters 11, 13, 15,18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51,53, and 55 provide the legal authority for operating the IBS components. IBS transmits Veteran records in order to administer statutory benefits programs to Veterans, Service members, reservists, and their spouses, surviving spouses, and dependents who file claims for a wide variety of benefits administered by VA.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (*Work with your System ISSO to complete this section)*

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

Principle of Purpose Specification: Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.

Principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program?

Principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual?

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

Follow the format below when entering your risk assessment:

Privacy Risk: Sensitive Personal Information (SPI), including personal contact, service, and benefits information could be released to unauthorized individuals.

Mitigation: IBS adheres to the information security requirements established by the VA Office of Information Technology (OIT):
• All employees with access to Veteran information are required to complete the VA Privacy and Information Security Awareness training and acknowledge the Rules of Behavior annually.
• The VBA applications listed in Section 1.4 and authorized VA staff only collect the information required to process Veteran inquiries regarding claims and benefits.
• Every individual with access to SPI are trained to adhere to Standard Operating Procedures (SOPs) for working with Veterans, entering data, and ensuring data is correct and complete.

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.

IBS facilitates Veteran/Beneficiary inquiries regarding their entitlements by retrieving information used to identify a Veteran (or Beneficiary), correspond with the Veteran, and inform the Veteran of their claims' status and benefits eligibility. The collected information includes:
• **Name**: Confirm Veteran's identity (internal and external)
• **Social Security Number:** Confirm Veteran's identity, create Veteran File Number, confirm Social Security Administration (SSA) benefits (internal and external)
• **Date of Birth:** Confirm Veteran's identity and benefits (internal and external)
• **Mother's Maiden Name:** Confirm Veteran's identity and benefits (internal)
• **Service Number:** Confirm Veteran's military service (internal)
• **Active service amount**: Determine Veteran's benefits (internal)
• **Branch of service:** Confirm Veteran's military service (internal)
• **Character of service:** Determine Veteran's benefits (internal)
• **Pay grade**: Determine Veteran's benefits (internal)
• **Assigned separation reason:** Determine Veteran's benefits (internal)
• **Service period:** Determine Veteran's benefits (internal)
• **Service-connected disabilities & diagnostics:** Determine Veteran's benefits (internal)
• **Reenlisted indication:** Determine Veteran's benefits (internal)
• **Purple Heart or other military decoration indication**: Determine Veteran's benefits (internal)
• **Date of death:** Confirm Veteran's identity and benefits
• **File Number**: Confirm Veteran's identity
• **Enlistment Date**: Confirm Veteran's military benefits

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

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

N/A

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.

Data are checked for completeness by system audits and manual verifications. Authorized VA staff can update data through IBS during Veteran correspondence using one of the applications described in Section 1.2, which validate entries using built-in rules for data format and possible values. All information is matched against supporting claims documentation, or DD-214 forms submitted by the

Veteran or Beneficiary. Additionally, certain data such as SSN are verified with the SSA. Prior to any award or entitlement authorizations by VBA, the Veteran record is manually reviewed, and data validated to ensure correct entitlement has been approved

2.3 How is the information in the system secured?

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

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

All apps are token authenticated to other apps to validate that requests are coming from validated sources for data in motion. This is done via built-in user authentication included in the BIP Framework.
All data at rest is housed in either CorpDB or the IBS RDS database. Connection information (including authentication passwords) for these are connections are secured via Vault.

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

SSN's are not part of the BIRLS ecosystem anymore. Removed in favor in file numbers.

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

Data is stored in a secure enclave within AWS. Access to information is protected by industry standard authentication and authorization protocols. Data is encrypted both in transit and at rest via SSL/TLS.

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?

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training, which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the ROB, the user must reaffirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system.

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

Yes

2.4c Does access require manager approval?

Yes

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

Yes

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

The Platform Accelerator teams control the security safeguards that are in all applications that use the BIP framework.

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*

Data is maintained indefinitely per VA data retention policies.
Data Elements retained i/c:

- Name
- Address
- Enlistment Date
- Date of Death
- File Number
- Social Security Number
- Birthdate
- Insurance Information
- Claim Data

3.2 How long is information retained?

In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. ***For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods****. The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented. If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

Data is maintained indefinitely per VA data retention policies.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

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

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

BIRLS follows the VA retention schedule, VHA Records Control Schedule 10-1, dated January 2020.

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.

The data is maintained indefinitely. No data elimination is required at this time.

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.

Test data is used during the design and development process. Access to PII in the production environment is controlled to specific VA systems.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

Follow the format below:

Privacy Risk: A potential risk of data leak may exist with retaining personal data

Mitigation: Controlled access to the data is maintained. Only those personnel required by job assignment have access to the data. Each employee with access to the data is required to attend data privacy training.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Benefits Delivery Network (BDN)	BDN is a suite of applications that collectively make up the VA's primary source of Compensation & Pension, Education, and Vocational Rehabilitation and Employment (VRE) information.	• Name • Social Security Number (SSN) • Date of Birth (DOB) • Service Number • Active service amount • Branch of service • Character of service • Pay grade • Assigned separation reason • Service period • Service-connected disabilities & diagnostics • Reenlisted indication • Purple Heart or other military decoration indication	Service-based
Corporate Database (CorpDB)	CorpDB provides Veteran service and identity information to make	• Name • SSN • DOB • Service Number	Service-based

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*
	compensation payments to Veterans because of Service-connected disabilities, or pension payments because of age, service-, or non-service-connected disabilities	• Active service amount • Branch of service • Character of service • Pay grade • Assigned separation reason • Service period • Service-connected disabilities & diagnostics • Reenlisted indication • Purple Heart or other military decoration indication	
Insurance Payment System (INS)	INS includes the Inforce subsystem to update information about living policyholders and process payments, as wells as the Awards subsystem to make payments to insurance beneficiaries. Provides Veteran Insurance information.	• Name • SSN • DOB	Service-based
Master Person Index (MPI)	MPI provides authoritative Veteran/Beneficiary identification information to confirm requestors' identities.	• Name • SSN • DOB • Mother's Maiden Name	Service-based
Veterans Benefits Management System (VBMS)	VBMS provides a paperless-based environment for claims processing, including establishment, development, rating, award, and appeal of a claim	• Name • SSN • DOB • Service Number • Active service amount • Branch of service • Character of service • Pay grade • Assigned separation reason • Service period • Service-connected disabilities & diagnostics	Service-based

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*
		• Reenlisted indication • Purple Heart or other military decoration indication	
VA/DoD Identity Repository (VADIR)	VADIR stores Veteran identity information, military history, payroll information, disabilities, and dependents (received from the Defense Enrollment Eligibility Reporting System (DEERS) to provide an electronic comprehensive view of Veteran eligibility and benefits utilization	• Name • SSN • DOB • Service Number • Active service amount • Branch of service • Character of service • Pay grade • Assigned separation reason • Service period • Service-connected disabilities & diagnostics • Reenlisted indication • Purple Heart or other military dec	Service-based

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: Personally Identifiable Information (PII), including personal contact, service, and benefits information could be released to unauthorized individuals.

Mitigation: IBS adheres to the access controls established by the VA Office of Information Technology (OIT) and the following security controls: Audit and Accountability, Security Assessment and Authorization, Incident Response, Personnel Security, and Identification and Authentication. All employees with access to Veteran information are required to complete the VA Privacy and Information

Security Awareness training and acknowledge the Rules of Behavior annually. Information is shared only in accordance with VA Handbook 6500.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program***	***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***	***List the method of transmission and the measures in place to secure data***

	office or IT system		***be more than one)***	
Social Security Administration (SSA)	Access to military discharge data	• Branch of Service • Pay Grade • DOB • Entered on Active Duty date (EOD) • Returned to Active Duty date (RAD) • File number • Claim number or SSN • Name • Date of Death • Character of Discharge • Total Active Service	Information Exchange Agreement #384 Section 205(a) of Social Security Act (Act) (42 U.S.C 405(a)) VA's System of Records (SOR) "Veterans and Beneficiaries Identification Records Location Subsystem-VA" (38VA21)	Electronic transmission methods in accordance with VA policy
National Archives and Records Administration (NARA)	Compare and confirm Veterans' historical records	• Name • SSN • DOB	Interconnection Security Agreement (ISA)/ Memorandum of Understanding (MOU)	Electronic transmission methods in accordance with VA policy
Department of Defense (DoD)	Provide Selective Service data requests	• Name • SSN • DOB	Interconnection Security Agreement (ISA)/ Memorandum of Understanding (MOU)	Electronic transmission methods in accordance with VA policy
Health and Human Services (HHS)	Confirm Federal Parent Locator Service data	• SSN • File number • Service Date • Date of Death	Interconnection Security Agreement (ISA)/ Memorandum of Understanding (MOU)	Electronic transmission methods in accordance with VA policy
Department of Education (ED)	Confirm Veteran education records data	• Name • SSN • DOB	Interconnection Security Agreement (ISA)/ Memorandum	Electronic transmission methods in accordance

			of Understanding (MOU)	with VA policy

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M06-16, note them here.

To protect Veteran PII, the following activities occur as part of the overall information assurance activities:
1. The information within each application is categorized in accordance with FIPS 199 and NIST SP 800-60, and all PII is identified as part of the categorization.
2. The VA has policies that direct and guide the activities and processes performed by the VA, which are periodically reviewed to ensure completeness and applicability.
3. The NIST SP 800-53 controls are selected based on the categorization. The controls provide protection for Veteran PII while developed or stored by an application or IT system, physically transported between facilities, stored offsite, or transmitted between IT centers.
4. Internal protection is managed by access controls such as user IDs and passwords, authentication, auditing, and internal network controls. Remote protection is provided by remote access control, authenticator management, auditing, and encrypted transmission.

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: PII, including personal contact, service, and benefits information could be released to unauthorized individuals. Additionally, misspelling a Veteran's name could result in the wrong data being displayed to the user.

Mitigation: Outside agencies provide their own level of security controls such as access control, authentication, and user logs in order to prevent unauthorized access. The ISA/MOUs between IBS and external agencies establish the security requirements for the VA and the external agency. The VA and external systems are protected by the Moderate system certification level which ensures criticality defined by FIPS 199. The authorization process is completed for IBS and external agencies, and an Authority to Operate (ATO) has been approved. The security controls identified by NIST SP 800-53 for a moderate system are implemented to protect IBS and external agencies.

All personnel with access to Veterans' information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior (ROB) annually. IBS users and applications adhere to all information security requirements established by VA OIT, and information is shared in accordance with VA Handbook 6500. All personnel accessing Veteran's information must first have a successfully adjudicated fingerprint check conducted by the Federal Bureau of Investigation (FBI). Individual users are given access to Veterans' data through the issuance of a user ID and password and using a Personal Identity Verification (PIV) card for two-factor authentication.

Section 6. Notice

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

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

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

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

58VA21 – Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA
45VA21 -Veterans Assistance Discharge System – VA
138VA005Q – Veterans Affairs Department of Defense Identity Repository (VADIR)- VA

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

N/A

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

Other VBA and external applications use IBS to transmit and collect Veteran data as needed. These systems are responsible for issuing notice of information collection.
The Department of Veterans Affairs provides public notice that the system exists in two ways:

1. The System of Record Notices (SORN) listed in the Federal Register:
    a. 45VA21: Veterans Assistance Discharge System-VA, http://www.gpo.gov/fdsys/pkg/FR2010-10-06/pdf/2010-25233.pdf

b. 58VA21/22/28: Compensation, Pension, Education, and Rehabilitation Records- VA, http://www.gpo.gov/fdsys/pkg/FR-2012-07-19/pdf/2012-17507.pdf
c. 138VA005Q: Veterans Affairs Department of Defense Identity Repository (VADIR) - VA, https://www.govinfo.gov/content/pkg/FR-2009-07-27/pdf/E9-17776.pdf

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

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.

Individuals have the right to decline providing information to VA personnel. However, failure to provide information may result in denial of access to health care benefits. Veterans and their family or guardian (spouse, children, parents, grandparents, etc.) may not decline or request their information not be included as part to determine eligibility and entitlement for VA compensation and pension benefits and also designate a guardian to manage the VA compensation and pension benefits.

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 VA compensation and pension benefits. The Privacy Act and VA policy require that PII information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Privacy Risk: Members of the public may not know that IBS exists within VA.

Mitigation: The VA mitigates this risk by providing the public with two forms of notice that the system exists, as identified in Section 6.1, including the System of Record Notice and Privacy Act statement.

Section 7. Access, Redress, and Correction

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

7.1 What are the procedures that allow individuals to gain access to their information?
These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

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

Those wishing to obtain more information about access, redress, and record correction of Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records, should contact the VA Regional Office as directed in the System of Record Notice (SORN) "VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA" 58VA21/22/28 (July 19, 2012). This SORN can be found online at: http://www.gpo.gov/fdsys/pkg/FR-2012-07-19/pdf/2012-17507.pdf.

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

N/A

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.

N/A

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Those wishing to obtain more information about access, redress, and record correction of Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records, should contact the VA Regional Office as directed in the System of Record Notice (SORN) "VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA" 58VA21/22/28 (July 19, 2012). This SORN can be found online at: http://www.gpo.gov/fdsys/pkg/FR-2012-07-19/pdf/2012-17507.pdf.

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.

Those wishing to obtain more information about access, redress, and record correction of Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records, should contact the VA Regional Office as directed in the System of Record Notice (SORN) "VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA" 58VA21/22/28 (July 19, 2012). This SORN can be found online at: http://www.gpo.gov/fdsys/pkg/FR-2012-07-19/pdf/2012-17507.pdf.

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.

Those wishing to obtain more information about access, redress, and record correction of Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records, should contact the VA Regional Office as directed in the System of Record Notice (SORN) "VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA" 58VA21/22/28 (July 19,

2012). This SORN can be found online at: http://www.gpo.gov/fdsys/pkg/FR-2012-07-19/pdf/2012-17507.pdf.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

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

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?
This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk: : Individuals may seek to access or redress their records 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. 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?

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.

Every five years, per VA Directive and Handbook 6330, VA OIT develops, disseminates, and reviews/updates a formal, documented policy that addresses purpose, scope, roles, responsibilities,

management commitment, coordination among organizational entities, and compliance; along with formal, documented procedures to facilitate the implementation of the control policy and associated controls.
OIT documents and monitors individual information system security training activities including basic security awareness training and specific information system security training and retains individual training records for 7 years. This documentation and monitoring are performed using the VA Talent Management System (TMS). Users of VA/VBA information systems gain access through an EO LAN control domain. The End Office (EO) Local Area Network (LAN) personnel use Group Policy Objects (GPO) to manage accounts, which is a set of rules that control the working environment of user accounts and computer accounts. The GPO provides the centralized management and configuration of operating systems, applications, and users' settings in an Active Directory environment. The GPO restricts certain actions that may pose potential security risks.

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?

N/A

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.

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.

There is a BIP NDA in place. It covers all personnel working on IBS.

The IBS development team is comprised of VA personnel and contractors. Access to IBS is required for system administrators and developers for day-to-day maintenance of the systems and networks. Review of access to IBS is performed on a quarterly basis by the Information System Owner (ISO) and the security engineer. Clearance is required for each person accessing the system. Contracts are reviewed annually by the Contracting Officer’s Representative (COR).

VA OIT provides basic security awareness training to all information system users (including managers, senior executives, and contractors) of VA information systems, or VA sensitive information as part of initial training for new users, when required by system changes, and annually thereafter.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training, which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the ROB, the user must reaffirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Not Yet Approved
2. *The System Security Plan Status Date:* N/A
3. *The Authorization Status:* Approved
4. *The Authorization Date:* 21-Dec-2022
5. *The Authorization Termination Date:* 21-Dec-2023
6. *The Risk Review Completion Date:* 21-Dec-2022
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* HIGH

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

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

Section 9 – Technology Usage

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

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

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

***Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1**. (Refer to question 3.3.1 of the PTA)*

Yes. IBS uses Veterans Administration Enterprise Cloud (VAEC) Cloud, this is a FedRAMP approved platform.

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

N/A

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

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

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

N/A

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

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

N/A

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

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

N/A

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

JEAN-CLAUDE WICKS

Digitally signed by JEAN-CLAUDE WICKS
Date: 2023.05.24 07:47:31 -06'00'

Privacy Officer, Jean-Claude Wicks

JOSEPH FACCIOLLI

Digitally signed by JOSEPH FACCIOLLI
Date: 2023.05.24 10:17:48 -04'00'

Information System Security Officer, Joseph Facciolli

Christina O. Lawyer 141790

Digitally signed by Christina O. Lawyer 141790
Date: 2023.05.24 10:39:00 -04'00'

Information System Owner, Christina Lawyer

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).

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

45VA21 -Veterans Assistance Discharge System – VA
https://www.govinfo.gov/content/pkg/FR-2010-10-06/pdf/2010-25233.pdf

138VA005Q – Veterans Affairs Department of Defense Identity Repository (VADIR)- VA
https://www.govinfo.gov/content/pkg/FR-2022-12-23/pdf/2022-27988.pdf

HELPFUL LINKS:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

VA Privacy Service Privacy Hub:

https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices