Privacy Impact Assessment for the VA IT System called:

VBA Automation Platform

VBA

Office of Business Integration (OBI)

eMASS ID # 1143

Date PIA submitted for review:

01/19/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Lakisha Wright	lakisha.wright@va.gov	202-632-7216
Information System Security Officer (ISSO)	Andrew Vilailack	andrew.vilailack@va.gov	813-970-7568
Information System Owner	Derek Herbert	Derek.Herbert@va.gov	202-461-9606

Abstract

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

The system, VBA Automation Platform (VBAAP) solution, brings together multiple technologies that work together to read and analyze information, make decisions, and take actions on veterans' claims for compensation. Technical components of VBAAP solution include Robotic Process Automation, Optical Character Recognition engine, Natural Language Processing, Business intelligence, Business Rules engine, data Ingestion and Management engine and so on.

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. What is the IT system name and the name of the program office that owns the IT system?

VBA Mail Automation Platform
VBA Office of Business Integration (OBI)

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

VBA Automation Platform system assists the Veterans Benefits Administration (VBA) with the triage and handling of mail associated with Veterans benefits claims (Veterans' Benefits Mail Automation Service (MAS)); Veterans' Benefits and Claim automation support services such as Veterans disability benefits claims processing (Additional Presumptive Capacity Automation Services (APCAS) Claim Automation, pension claim processing (Pension Optimization Initiative (POI), Private medical records (PMR), National Cemetery (NCA) and DoJ Records.

C. Who is the owner or control of the IT system or project?

The VBA Automation Platform (VBAAP) IT system/environment is provided by IBM Intelligent Automation Platform (IBM IAP) as a managed service to VA VBA's Office of Business Integration (OBI).

2. Information Collection and Sharing

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

VA systems acquires data from Veterans. VBAAP acts only as a data processor. And the processed data is stored back in the VA systems. The number of individuals/veterans the VBAAP system processes is nearly 6,787,884.

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

The VBA Automation Platform is a managed service that uses unattended automation to assist the Veterans Benefits Administration (VBA) with the triage and handling of mail associated with Veterans benefits claims (Veterans' Benefits Mail Automation Service (MAS)), Veterans disability benefits claims processing (Additional Presumptive Capacity Automation Services (APCAS) Claim Automation) and pension claim processing (Pension Optimization Initiative (POI), Private medical records (PMR), National Cemetery (NCA) and DoJ Records. The unattended automation consists of direct system to system integration and robotic process assist (RPA) technology. VBA employees provide the business rules and oversight needed.

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

The information sharing conducted by the VBA Automation Platform includes PII and PHI such as –

- *Name*
- *Social Security Number*
- *Date of Birth*
- *Personal Mailing Address*
- *Personal Phone Number*
- *Personal fax number*
- *Personal Email Address*
- *Emergency Contact Information*
- *Financial Information*
- *Health Insurance beneficiary Number*
- *Certificate/License Number*
- *Medications*
- *Race*
- *Tax Identification Number*
- *Medical Record Number*
- *Gender*
- *Integrated Control Number*
- *Military History/Service Connection*
- *Next of Kin*
- *Date of Death*
- *Dependent Information*
- *Marital Information*
- *Income/Expense Information*
- *Social Security Benefit Information*
- *Federal Tax Information*
- *VA Pension Benefit Information*
- *Clinical Data*
- *Service Connectivity Data*
- *Mailing Address*
- *Zip code*
- *Account Numbers*
- *Current Medications*
- *Previous Medical Records*
- *Claims attributes such as Flashes, Contentions, Special Issues*
- *Claims Documents (such as Private and Federal Medical Records; Benefit entitlement and administrative records)*
- *Claims Decision*
- *FileNumber*
- *Queue*
- *AssignedTo*
- *PacketId*
- *Update award information*
- *Update rating information*
- *Request Military Service Records*
- *Clinical data including medical conditions, diagnostics, treatment, medication, medical notes*
- *Claimant Name*
- *Cause of Death*
- *Claim information*

The key modules/components of the IBM IAP solution providing VBAAP services include:

1. Robotic Process Automation
2. Intelligent OCR
3. AI / NLP Technologies
4. Business Process Management
5. Business Intelligence
6. Identity & Access management

G. Is 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?

No, the system is hosted at only one AWS GovCloud West location

3. Legal Authority and SORN

H. What is the citation of the legal authority to operate the IT system?

VBA Office of Business Integration (OBI)
Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records- VA (SORN) # 58VA21/22/28

The authority for the United States Department of Veterans Affairs (VA) to collect and share data for the purpose outlined under the project scope include:

- Privacy Act of 1974, 5 U.S.C. § 552a, as amended
- VA Claims Confidentiality Statute, 38 U.S.C § 5701

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

No, system is not in the process of being modified so the SORN will not require amendment or revision and approval

4. System Changes

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

No

K. Will the completion of this PIA could potentially result in technology changes?

No

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. It must also match the information provided in question 3.4 of the PTA.

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

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☒ Personal Fax Number
- ☒ Personal Email Address
- ☒ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☒ Financial Information
- ☒ Health Insurance Beneficiary Numbers Account numbers
- ☒ Certificate/License numbers[1]
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☒ Medications
- ☒ Medical Records
- ☒ Race/Ethnicity
- ☒ Tax Identification Number
- ☒ Medical Record Number
- ☒ Gender
- ☒ Integrated Control Number (ICN)
- ☒ Military History/Service Connection
- ☒ Next of Kin
- ☒ Other Data Elements (list below)

Other PII/PHI data elements: <<Add Additional Information Collected but Not Listed Above Here (For Example, A Personal Phone Number That Is Used as A Business Number)>>

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

- Date of Death
- Dependents
- Marital Information – Dates etc.
- Income
- Expenses
- Social Security Benefits
- Federal Tax Information
- VA Pension Benefits
- Email ID
- Clinical data,
- Service connectivity data
- FileNumber
- Queue
- AssignedTo
- PacketId
- Update award information
- Update rating information
- Claimant Name
- Cause of Death
- Claim information
- Claims attributes such as Flashes, Contentions, Special Issues
- Claims Documents (such as Private and Federal Medical Records; Benefit entitlement and administrative records)
- Claims Decision

PII Mapping of Components (Servers/Database)

VBAAP consists of **11** key components (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **VBAA** and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards

VBA Automation Platform	Yes	Yes	Name, SSN, DOB, Address, Phone, Fax number, Veteran Health Records, Federal Tax Information	To be able to provide Benefits Automation services for the veterans	NIST SP 800-53 Controls; VA Handbook 6500; DoD DISA STIGs; FIPS 140-2 encryption
Appian	Yes	Yes	Name, SSN, DoB, Address, Phone, Medical Health Records (PHI), Federal Tax Information (FTI)	To orchestrate the workflow process, provide data service to access database and temporary storage for downloaded forms and documents.	Data encryption at rest using storage level encryption. Data encryption in motion using TLS1.2 for all web services to interact with system components. Plus NIST SP 800-53 Controls; VA Handbook 6500
Blue Prism	Yes	No	Name, SSN, DoB, Address, Phone, Medical Health Records(PHI)	To automate the identification, triage, download forms from the Mail Portal and make updates to the VBMS system. No data is stored in BluePrism.	No data is stored in Blue Prism. Data encryption in motion using TLS1.2 for all web services to interact Plus NIST SP 800-53 Controls ; VA Handbook 6500
SQL Database	Yes	Yes	Name, SSN, DoB, Address, Phone etc.	To make the data accessible for different components of the system to process the data. To maintain audit	Data encryption at rest and in motion. Data storage disks are encrypted. Only

				data to investigate and resolve any data processing issues.	authorized uses will have access to the database. All access to database using TLS1.2 based services which ensure data encryption in motion. Plus NIST SP 800-53 Controls; VA Handbook 6500
Watson ACD	Yes	No	Clinical Data	To analyze the clinical data to look for presumptive conditions.	It is a stateless service, and it does not store or track any clinical data besides analysis of the input. Plus NIST SP 800-53 Controls ; VA Handbook 6500
UiPath	Yes	No	Name, SSN, DoB, Address, Phone etc.	To automate the identification, triage, download forms from the Mail Portal and make updates to the VBMS system. No data is stored in BluePrism.	Data encryption in motion using TLS1.2 for all web services to interact with other systems. Plus NIST SP 800-53 Controls ; VA Handbook 6500
Document DB – NOSQL Database	No	Yes	Name, SSN, DoB, Address,	To make the data accessible	Data encryption in

			Phone, clinical data, service connectivity data etc.	for different components of the system to process the data. To maintain audit data to investigate and resolve any data processing issues.	motion using TLS1.2 for all web services to interact with other systems. Plus NIST SP 800-53 Controls ; VA Handbook 6500
PMR Concord eFAX	Yes	No	Name, SSN, DoB, Address, Phone, clinical data etc.	Sends secure electronic fax to private medical providers.	Data encryption in motion using TLS1.2 for all web services to interact with other systems. Plus NIST SP 800-53 Controls ; VA Handbook 6500
S3 Buckets/EFS	No	Yes	Name, SSN, DoB, Address, Phone, clinical data, service connectivity data	Stores data in AWS GovCloud for short-term/long-term use	FedRAMP High AWS Gloud security and compliance controls
Databricks	No	Yes	Name, SSN, DoB, Address, Phone, clinical data, service connectivity data	To transform, augment, and cleanse VBA Automation platform databases	Data encryption in motion using TLS1.2 for all web services to interact with other systems. Plus NIST SP 800-53 Controls ; VA Handbook 6500
Neo4j	No	Yes	Name, SSN, DoB, Address, Phone, clinical data, service	To utilize graph database capabilities to better define,	Data encryption in motion using TLS1.2 for all

			connectivity data	discover, and store data and data relationships, and providing high speed query capabilities across the graph database.	web services to interact with other systems. Plus NIST SP 800-53 Controls ; VA Handbook 6500

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?

Information is collected from the VA Centralize Mail Portal, Veteran's Benefits Management System (VBMS), VBMAS-A, VBMS-R, Corporate Data warehouse, Caseflow, CAPRI, Lighthouse, VISTA/HDR, eFolder, SCIP, SSA, IRS and the VA Master Person Index (MPI) for verification of the data received on the intake forms and to automate the processing of claims.

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.

N/A

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

Reports of claims processed, the source of information is the Centralized Mail Portal.

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?

Information is collected using standard Application Programming Interfaces (API)s and front-end automation leveraging Robotic Process Automation (RPA) technologies

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

N/A

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.

The information will be checked using number of different methods –

1. Using Optical Character Recognition (OCR) /Intelligent Character Recognition (ICR). The confidence level of extraction from each method is evaluated and the results with the highest level of confidence are used.

2.Data is validated against VA source systems. If the identifying information does not match, then the data is not processed any further. 3. Artificial Intelligence models are used to classify some data elements, which cannot be accurately extracted with high level of confidence by the OCR/ICR Process. 4. Data which cannot be accurately extracted and validated by the above methods are off ramped for humans to process

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

No commercial aggregators used.

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

Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records- VA (SORN) # 58VA21/22/28

The authority for the United States Department of Veterans Affairs (VA) to collect and share data for the purpose outlined under the project scope include:

- Privacy Act of 1974, 5 U.S.C. § 552a, as amended
- VA Claims Confidentiality Statute, 38 U.S.C § 5701

Additionally, a fully executed ISA-MOU governs the interconnections between the VA and IBM the IBM Automation system (VBAAP) via the FIPS140-2 cryptographic module.

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 Individual Information (SII), Personal Health Information (PHI), and Personally Identifiable Information (PII) data is stored in the system that could be compromised if appropriate safeguards are not in place.

Mitigation: The IBM IAP environment serving VBA Automation Platform is hosted on AWS GovCloud which is FedRAMP High Cloud environment with most stringent data security and privacy safeguards in place as part of maintaining their FedRAMP High certification. Additionally, the VBAAP system adheres to FISMA-Moderate Security & Compliance ATO requirements using VA handbook 6500 and NIST SP 800-53r4 controls, protecting Confidentiality, Integrity and Availability of the data and the system.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
Name	To establish and process disability, pension, and benefits claims	Not used
SSN	To establish and process disability, pension, and benefits claims	Not used
Date of Birth	To establish and process disability, pension, and benefits claims	Not used
Personal Mailing Address	To establish and process disability, pension, and benefits claims	Not used
Personal Phone Number(s)	To establish and process disability, pension, and benefits claims	Not used
Personal Fax Number	To establish and process disability, pension, and benefits claims	Not used
Personal Email Address	To establish and process disability, pension, and benefits claims	Not used
Emergency Contact Information	To establish and process disability, pension, and benefits claims	Not used
Financial Information	To establish and process disability, pension, and benefits claims	Not used
Health Insurance Beneficiary Numbers Account numbers	To establish and process disability, pension, and benefits claims	Not used
Certificate/License numbers	To establish and process disability, pension, and benefits claims	Not used
Medications	To establish and process disability, pension, and benefits claims	Not used
Integrated Control Number (ICN)	To establish and process disability, pension, and benefits claims	Not used
Military History/Service Connection	To establish and process disability, pension, and benefits claims	Not used
Next of Kin	To establish and process disability, pension, and benefits claims	Not used
Beneficiary Information	To establish and process disability, pension, and benefits claims	Not used
Federal Tax Information (FTI)	To establish and process disability, pension, and benefits claims	Not used
Race	To establish and process disability, pension, and benefits claims	Not used
Gender	To establish and process disability, pension, and benefits claims	Not used
Date of Death	To establish and process disability, pension, and benefits claims	Not used

Marital Information	To establish and process disability, pension, and benefits claims	Not used
VA Pension Benefits Information	To establish and process disability, pension, and benefits claims	Not used
Medical Health Records	To establish and process disability, pension, and benefits claims	Not used
Address	To establish and process disability, pension, and benefits claims	Not used
Phone	To establish and process disability, pension, and benefits claims	Not used
Fax Number	To establish and process disability, pension, and benefits claims	Not used
Clinical data	To establish and process disability, pension, and benefits claims	Not used
Service connectivity data	To establish and process disability, pension, and benefits claims	Not used
Date of Death	To establish and process disability, pension, and benefits claims	Not used
Dependents	To establish and process disability, pension, and benefits claims	Not used
Marital Information	To establish and process disability, pension, and benefits claims	Not used
Income	To establish and process disability, pension, and benefits claims	Not used
Expenses	To establish and process disability, pension, and benefits claims	Not used
Social Security Benefits	To establish and process disability, pension, and benefits claims	Not used
Federal tax Information	To establish and process disability, pension, and benefits claims	Not used
VA pension Benefits	To establish and process disability, pension, and benefits claims	Not used
FileNumber	To establish and process disability, pension, and benefits claims	Not used
Queue	To establish and process disability, pension, and benefits claims	Not used
AssignedTo	To establish and process disability, pension, and benefits claims	Not used
PacketId	To establish and process disability, pension, and benefits claims	Not used
Update award information	To establish and process disability, pension, and benefits claims	Not used
Update rating information	To establish and process disability, pension, and benefits claims	Not used

Claimant Name	To establish and process disability, pension, and benefits claims	Not used
Cause of Death	To establish and process disability, pension, and benefits claims	Not used
Claim information	To establish and process disability, pension, and benefits claims	Not used
Claims attributes such as Flashes, Contentions, Special Issues	To establish and process disability, pension, and benefits claims	Not used
Claims Documents (such as Private and Federal Medical Records; Benefit entitlement and administrative records)	To establish and process disability, pension, and benefits claims	Not used
Claims Decision	To establish and process disability, pension, and benefits claims	Not used

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.

- Robotic Process Automation
- Intelligent OCR
- Business Process Engine
- AI / NLP Technologies
- Business Intelligence

PII and PHI data associated with claims are analyzed using the above tools and benefit decision is produced and updated on the VA systems.

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?

VBAAP analyzes a large amount of unstructured data using Natural Language Understanding/ Processing techniques to make benefit decisions.

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.

The VBAAP system/solution adds newly derived information to the claim record which will enable the government employee to make benefit decision based on available evidences.

2.3 How is the information in the system secured?

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

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

The measures that are in place to protect data in transit and data at rest include - FIPS 140-2 cryptographic encryption on storage and backups, TLS 1.2 or better on all webservers and strict access controls/ACLs.

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

Additional safeguards are in place to protect SSNs and minimize the exposure and misuse by implementing strict role-based access controls, multi-factor authentications and layered security including VPN, private subnets, firewalls, bastion hosts and encryption at all possible levels

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

In accordance with OMB Memorandum M-06-15 the PII/PHI data in the environment is safeguarded using multi-layer-security and defense-in-depth approach that include program level adherence to FISMA/FedRAMP controls and security best practices such as role-based access controls, multi- factor authentications, VPN, private subnets, firewalls, bastion hosts and encryption at all possible levels.

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?

All roles/users/administrators of VBA Automation Platform system are vetted through eQIP clearance process and are required to use VA PIV smart card to access VA environment. User roles and responsibilities and entitlements are strictly monitored, tracked, and managed by the system owners and the managers. The VBA Automation Platform collects and uses minimum required PII and uses the VA handbook 6500 based FISMA Moderate Risk Management Framework to safeguard the system and the data that is being handled as part of the VBA Automation Platform solution. This is in adherence to the requirements depicted in the contract PWS.

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 VBA Automation Platform's Program Director and the VA Information System Owner are ultimately responsible for assuring safeguards for the PII data in the environment. All supporting teams such as PMO, Security, DevSecOps are required to follow those safeguards at every possible step throughout the solution delivery cycles.

Section 3. Retention of Information

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

3.1 What information is retained?

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

The VBA Automation Platform only processes the PII and PHI information sourced from VA systems. The data is not retained beyond 6 months post processing.
The list of data elements that are retained include:

- Name
- *Social Security Number*
- *Date of Birth*
- *Personal Mailing Address*

- *Personal Phone Number*
- *Personal fax number*
- *Personal Email Address*
- *Emergency Contact Information*
- *Financial Information*
- *Health Insurance beneficiary Number*
- *Certificate/License Number*
- *Medications*
- *Race*
- *Tax Identification Number*
- *Medical Record Number*
- *Gender*
- *Integrated Control Number*
- *Military History/Service Connection*
- *Next of Kin*
- *Date of Death*
- *Dependent Information*
- *Marital Information*
- *Income/Expense Information*
- *Social Security Benefit Information*
- *Federal Tax Information*
- *VA Pension Benefit Information*

3.2 How long is information retained?

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

The VBAAP system retains the data during the claims & benefits processing phase for about six months. VBAAP discards the data from databases once it is sent to cold storage.

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

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

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

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

Not Applicable. While the VBA Automation Platform processes veteran's mail, and analyses existing data for presumptive conditions, it does not generate records per the definition of a record by the VA records office and NARA

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

Not Applicable. While the VBA Automation Platform processes veteran's mail, and analyses existing data for presumptive conditions, it does not generate records per the definition of a record by the VA records office and NARA. The VBA Automation Platform processes packets in the mail portal and ensures that the correct actions are input into VBMS while also uploading the source documents from the mail portal into VBMS, which is the system of record for benefits information. Pension automation does not generate any additional data beyond mail automation. Presumptive condition uses existing data to evaluate eligibility for presumptive condition. No additional data is generated for any of these systems.

The VBA Automation platform will adhere to General Records Schedule 3.2 (GRS 10, 20, 30) in order to ensure the security of information technology systems and data, as well as the ability to respond to any computer security incidents that occur.

https://www.archives.gov/files/records-mgmt/grs/grs03-2.pdf

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.

Since all data is stored in the AWS GovCloud storage solution, IBM IAP/VBAAP environment will depend on AWS GovCloud for data handling, retention, and disposal requirements as per the FedRAMP and NIST SP 800-88 compliance guidelines. In general, the VBAAP system will adhere to VA Handbook 6500 and FISMA Moderate controls for all data processing activities.

All locally/temporarily stored data during data-processing activities by VBAAP, will be purged according to the customer specified timelines by using an automated script which will programmatically delete old data from the tables.

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.

Access to all the VBA Automation Platform environments and visibility to PII data is strictly controlled and available only to the VBAAP staff that holds PIV/HSPD-12 clearance and has a need-to-know based on their role in the environment.

VBA Automation Platform uses data strictly as per the contract/PWS and does not share the PII data with any other entities and does not use PII data for any training purposes.

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: As part of the Mail Automation service, VBA Automation Platform will be processing Veterans' mails that may contain PII and other sensitive data fields.

Mitigation: Since all data is stored in the AWS GovCloud storage solution, IBM IAP/VBAAP environment will depend on AWS GovCloud for data handling, retention, and disposal requirements as per the FedRAMP and NIST SP 800-88 compliance guidelines. No PII or SPI will be locally stored in the VBA Automation Platform permanently.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Veterans Benefits Administration Veterans Benefit Management System (VBMS)	To use the automated information towards veterans' Claims & Benefit Processing	Social Security Number, File Number, Name, Benefits Information, Dependent Information, Claims Decision, Claims attributes such as Flashes, Contentions, Special Issues	Web Application access over Hypertext Transfer Protocol Secure (HTTPS) Business Partner Extranet (BPE)
Veteran Benefits Administration Digitized Mail Handling Services (DMHS)	To use the electronic mail packet information towards veterans' Claims & Benefit Processing	Social Security Number, FileNumber, Name, Address, Mail Packet (forms and evidence documents)	Web Application access over HTTPS Mutual SSL connection
Veteran Benefits Administration BGS Web Services	BGS Web Services	Social Security Number, FileNumber, Benefits Information, Claim information, Dependent information.	Simple Object Access Protocol (SOAP) over HTTPS

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*
			Business Partner Extranet (BPE)
Veteran Benefits Administration VBMS Web Services	VBMS Web Services	Social Security Number, FileNumber, Name, Address, Documents (such as Private and Federal Medical Records; Benefit entitlement and administrative records)	SOAP over HTTPS Business Partner Extranet (BPE)
Veteran Benefits Administration DMHS Tableau Reports	DMHS Tableau Reports	File Number, Name, Queue, AssignedTo, PacketId	Secure File Transfer Protocol (SecureFTP)
Veteran Benefits Administration eFolder	Electronic documents associated with the veteran	Social Security Number, FileNumber, Name, Address, Documents	Web Application access over HTTPS
Veteran Benefits Administration VBMS-A	Update award information	Update award information	Web Application access over HTTPS
Veteran Benefits Administration VBMS-R	Update rating information	Update rating information	Web Application access over HTTPS
Veteran Benefits Administration STR	Request Military Service Records	Request Military Service Records	Web Application access over HTTPS
Master Person Index	Veteran data is received to validate the intake	Veteran Name, Address, DoB, SSN, Veteran File Number, Claimant Name, Address etc.	Standard APIs provided by VA, over Site-to-site VPN tunnel
P&F	Data extracted from certain forms	Veteran Name, Address, DoB, SSN, Veteran File Number, Claimant Name, Address, Date of Death, Cause of Death etc.	Standard APIs provided by VA over Business Partner Extranet (BPE)
Standards and COTS Integration Platform (SCIP)	To evaluate presumptive conditions	Clinical data including medical conditions, diagnostics, treatment, medication, medical notes etc.	REST APIs over BPE

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*
Heath Data Repository (HDR)	To evaluate presumptive conditions	Clinical data including medical conditions, diagnostics, treatment, medication, medical notes etc.	REST APIs over BPE
Veterans Health Administration Lighthouse	To evaluate presumptive conditions	Clinical data including medical conditions, diagnostics, treatment, medication, medical notes	REST APIs over BPE
Veterans Health Administration CAPRI	To evaluate presumptive conditions	Clinical data including medical conditions, diagnostics, treatment, medication, medical notes	CAPRI thick client Interface
Veterans Benefits Administration Caseflow	To access past rating decisions and create new	Social Security Number, File Number, Name, Benefits Information, Dependent Information, Claims Decision, Flashes, Contentions, Special Issues	Web Application access over HTTPS
Veterans Benefits Administration Benefits Integration Platform	To share extracted and processed claim information	Social Security Number, File Number, Name, Benefits Information, Dependent Information, Claims Decision, Flashes, Contentions, Special Issues	Standard APIs provided by VA Over BPE
Veterans Benefits Administration Lighthouse Delivery Infrastructure	To share claims data for processing	Social Security Number, File Number, Name, Benefits Information, Dependent Information, Claims Decision, Flashes, Contentions, Special Issues	REST APIs
Veterans Benefits Administration Performance, Analytics and Information (PA&I)	To share certain type of claims' extracted information for analysis	Social Security Number, File Number, Benefits Information, Claim information, Dependent information.	SFTP
VA Notify	To send secure email notification to veterans and claimants.	Social Security Number, File Number, Benefits Information, Claim information, Dependent information	REST APIs over BPE
Concord eFax	To send medical records requests to Private Medical	Social Security Number, Date of Birth, Name, Address, Medical condition	REST APIs over BPE

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*
	Providers through electronic fax.		
EOAS	To process Pre-burial claims	Social Security Number, Date of Birth, File Number, Benefits Information, Claim information, Dependent information	Web Application access over HTTPS
WebPMC	To process Presidential Memorial Certificate	Social Security Number, File Number, Benefits Information, Dependent information, Date of Birth, Date of Death	Web Application access over HTTPS

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: The data that is shared with other VA internal organizations, such as VBMS and DMHS may contain PII and other sensitive data.

Mitigation: The VA organizations such as VBMS, DMHS, PF&S who will be receiving the automated mail packets data, veterans' benefits claim data, and/or pension optimization data from the VBA Automation Platform(VBAAP) do have their own agency ATOs or Security and Privacy controls in place that govern their use of this system and data in accordance with VA Handbook 6500 RMF and NIST publications.

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***
DOJ	Helps to streamline the discovery process for the Camp Lejeune Justice Act of 2022, where in	All veteran records in VA's efolder (which may contain PII and PHI) such as: • Name • Social Security Number • Date of Birth • Mailing Address • Zip Code • Phone Number(s) • FaxNumber	N/A	Web Application access over HTTPS

	VA and DOJ users request records for a list of litigants and the application fetches relevant documents from efolder and provides a ZIP file that includes a summary document along with all of the litigants eFolder documents for each record request.	• EmailAddress • Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Financial AccountInformation • Health Insurance Beneficiary Numbers • Account numbers • Current Medications • Previous Medical Records • Race/Ethnicity		

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

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

Follow the format below:

Privacy Risk: PII/PHI data could be compromised if appropriate safeguards are not in place.

Mitigation: – DOJ Records request application has segregated data access controls in place to restrict the data visibility and sharing. Users are on-boarded after VA vetting and approval process and periodic validations of account and audits are in place.

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.

The IBM IAP/VBAAP system is not collecting information directly from individuals but from other VA systems and those systems cover notice in their own PIAs.

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

The IBM IAP/VBAAP system is not collecting information directly from individuals but from other VA systems and those system owners would need to provide the copy of current notice, if any.

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.

N/A – The IBM IAP/VBAAP system is not collecting information directly from individuals but from other VA systems. IBM IAP does not interface with the end users directly and has no role in informing veterans or stakeholders.

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.

N/A – The IBM IAP/VBAAP system does not collect information directly from individuals

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.

N/A – The IBM IAP/VBAAP system is not collecting information directly from individuals but from other VA systems. IBM IAP has no role in consent forms process.

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: The veterans may be unaware of how their mail and other benefits data is handled and what their privacy rights are.

Mitigation: This risk is mitigated through some of the steps listed below:

IBM IAP/VBA Automation Platform does not collect any veteran data. All veteran mail and other benefits data is provided to IBM IAP Platform by VA and is governed by the contract between VA and IBM. IBM is VA's Managed Services provider contractor.

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.***

IBM IAP/VBAAP is not an end-user facing system.

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. This system only processes information and updates the appropriate VBA systems of record

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 – This is not a system of record, or collection of information from Veterans, the system only processes information and updates the appropriate VBA systems of record. The Automation Platform is not collecting information directly from individuals.

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.

N/A –The Automation Platform is not collecting information directly from individuals but from other VA systems and those systems would cover the veterans' access/redress/and correction related issues.

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.

N/A –The Automation Platform is not collecting information directly from individuals but from other VA systems and those systems would cover the veterans' access/redress/and

correction related issues. IBM IAP/VBAAP system has no role or authority to interact with individual veterans/users.

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.

N/A –The Automation Platform is not collecting information directly from individuals but from other VA systems and those systems would cover the veterans' access/redress/and correction related issues. IBM IAP/VBAAP system has no role or authority to interact with individual veterans/users.

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: N/A

Mitigation: N/A

Section 8. Technical Access and Security

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

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

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

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

Only the IBM IAP team and the VBA employees assigned to this project are given access to the VBA Automation Platform systems and data after these users are fully vetted through the eQIP clearance process. The VA COR, managers/system owners assign, track and monitor every user account, their roles and responsibilities and user life-cycle. For every role, Separation of Duties (SoD) and Least Privilege rules are applied in order to ensure that access to PII is restricted only

to those who have a business need to use it. Roles are limited since there aren't traditional users of the system.

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?

Small group of DOJ users have access to DOJ-Record Request web application in the system to support the CampLejeune Justice Act of 2022, where in the vetted DOJ users are provided access to electronic records of veteran's identified by VA

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.

The VA COR, managers/system owners assign, track and monitor every user account, their roles and responsibilities and user life-cycle. All user accounts are VBAAP system users and are not traditional end users. For every role, Separation of Duties (SoD) and Least Privilege rules are applied in order to ensure that access to PII is restricted only to those who have a business need to use it. No regular user accounts are created on this system, since this system provides only the robotic processing automation (no human intervention) for the Benefits and other processes and workflows.

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.

IBM IAP, the managed services provider for VA's VBA Automation Platform, ensures that there are NDAs/BAAs in place with any Third-Party contracting organizations that are part of the overall VBAP systems and solution.

IBM IAP/VBAAP system is hosted on AWS GovCloud and that CSP account governs the vendor risk management processes. IBM and VA have a PWS and ISA-MOU in place.

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

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

All users of the VBA Automation Platform are provided the VA Privacy Information Security (PISA) training and VA Information Security Rules of Behavior (RoB) prior to gaining access to any VA information system or sensitive information. Additional trainings role-based trainings may also get assigned based on role of a user. Annual recertification is required for all trainings.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* <<ADD ANSWER HERE>>
2. *The System Security Plan Status Date:* <<ADD ANSWER HERE>>
3. *The Authorization Status:* <<ADD ANSWER HERE>>
4. *The Authorization Date:* <<ADD ANSWER HERE>>
5. *The Authorization Termination Date:* <<ADD ANSWER HERE>>
6. *The Risk Review Completion Date:* <<ADD ANSWER HERE>>
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* <<ADD ANSWER HERE>>

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.***

Yes.

The Security Plan Status - Operational
The Security Plan Status Date – 01/08/2024
The Authorization Status – ATO granted
The Authorization Date – 03/02/2023
The Authorization Termination Date – 03/02/2024
The Risk Review Completion Date – Underway, January 2024
The FIPS 199 classification of the system (LOW/MODERATE/HIGH) - MODERATE

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, the IBM IAP/VBAAP system uses Cloud technology and is hosted on AWS GovCloud. The AWS GovCloud Cloud services provider (CSP) has a FedRAMP agency authorization. And the VBAAP Managed Services has FISMA Moderate agency ATO that adheres to NIST and VA Handbook 6500 controls. The AWS GovCloud is a IaaS model while the IBM IAP managed service is a PaaS and SaaS model.

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.*

CSP AWS GovCloud – FedRamp High, FedRAMP
IBM-VA Automation Platform Package ID: F1603047866

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.

Yes.
AWS GovCloud, as a CSP has access and ownership to ancillary data.

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.

AWS is a CSP. AWS would be able to provide more details about the CSP responsibility matrix, data collected and controls information. The CSP contract/account abides with FedRAMP High security, privacy, compliance and accountability requirements as a condition to maintain their FedRAMP High certification. As a business owner of the data that is hosted in this environment, VA has the ultimate responsibility and accountability towards safeguarding veterans' data.

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).

Yes, the IBM IAP/VBAAP is utilizing Robotic Process Automation (RPA) tools to automate VBA processes by integrating with VA systems.

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

ID	Privacy Controls
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.

LAKISHA WRIGHT

Digitally signed by LAKISHA WRIGHT
Date: 2024.03.19 07:28:35 -04'00'

Privacy Officer, Lakisha Wright

ANDREW VILAILACK

Digitally signed by ANDREW VILAILACK
Date: 2024.03.19 12:39:14 -04'00'

Information System Security Officer, Andrew Vilailack

DEREK HERBERT

Digitally signed by DEREK HERBERT
Date: 2024.03.22 09:18:11 -04'00'

Information System Owner, Derek Herbert

APPENDIX A-6.1

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

HELPFUL LINKS:

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

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

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

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

Notice of Privacy Practice (NOPP):
VHA Notice of Privacy Practices
VHA Handbook 1605.04: Notice of Privacy Practices