Privacy Impact Assessment for the VA IT System called:

Benefits Integration Platform (BIP)

Veterans Benefits Administration (VBA)

Office of Business Integration (OBI)

eMASS ID# 2859

Date PIA submitted for review:

06/16/2025

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Marvis Harvey	Marvis.Harvey@va.gov	(314) 964-5469
Information System Security Officer (ISSO)	Joseph Facciolli	Joseph.Facciolli@va.gov	(215) 842-2000 ext. 2012
Information System Owner	Tushar Dode	Tushar.Dode@va.gov	(703) 930-7609

Abstract

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

The Benefits Integration Platform (BIP) provides a container-based application platform in the VA Enterprise Cloud (VAEC) Amazon Webservice (AWS) GovCloud that allows teams supporting Veterans Benefits Administration (VBA) and National Cemetery Administration (NCA) to develop, deploy, scale, secure, and manage container-based applications in a multi-tenant cloud environment quickly and easily. This supports VBA's mission to provide Veteran benefits in a timely, secure, and scalable manner.

BIP leverages Amazon Elastic Kubernetes Service (EKS) and Amazon Elastic Container Service (ECS) clusters for container management and orchestration, which allows teams to develop, scale, and deliver modern, secure, and properly segmented (from a storage, network, and compute perspective) applications in a multi-tenant environment. The AWS Virtual Private Clouds (VPCs) within BIP are sequentially peered to allow connectivity between VPCs, which supports the promotion of container images from lower VPCs to higher VPCs. The peering is essential for DevOps and Agile methodologies and secured allowing only container images to be mirrored between registries in each VPC. BIP also leverages a suite of VA Technical Reference Model (TRM) approved commercial-off-the-shelf (COTS) tools (e.g., Jenkins, Prisma Cloud, Vault, Nexus, Consul) to help development teams deliver quickly and effectively. In addition, BIP, as a General Support Systems (GSS), will further support VA minor application tenants by constraining the NIST 800-53 Rev. 4 controls necessary for applications hosted on the platform.

BIP stores data in the FTI Data S3 data store within the FTI Secure Enclave and the Fraud Prevention RDS Database. BIP retains IRS data, received via the Benefits Enterprise Platform (BEP), with the FTI Data S3 data store within the FTI Secure Enclave. The Fraud Prevention DB contains PII used in support of claims processing. Minor/Tenant applications provide, and are responsible for, any data retained in support of their individual mission.

Overview

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

1 General Description

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

BIP provides a container-based application platform in the VAEC AWS GovCloud that allows teams supporting VBA and NCA to develop, deploy, scale, secure, and manage container-based applications in a multi-tenant cloud environment quickly and easily. This supports VBA's mission to provide Veteran benefits in a timely, secure, and scalable manner.

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

BIP is owned by the VBA OBI and operated by the Benefits Integration and Administration (BIA) Product Line (PL), which is situated within the Benefits and Memorial Services (BAM) Portfolio.

2. Information Collection and Sharing

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

BIP processes information regarding Veterans, Dependents, VA Employees and VA Contractors. The expected number of individuals whose information is stored in the system is 51.4 million.

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

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

BIP processes Veteran information in support of claims processing on behalf of minor/tenant applications.

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

BIP processes Veteran information in support of claims processing on behalf of minor/tenant applications. BIP stores Veteran and dependent information data in the form of documents stored in the FTI Data S3 data store within the FTI Secure Enclave and the

Fraud Prevention RDS Database. IRS document data, received via BEP with the FTI Data S3 data store within the FTI Secure Enclave. The Fraud Prevention DB contains PII used in support of identifying instances of fraud, waste, and abuse with Veteran payments. BIP components, BIP Fiduciary Service and Benefits Integration Events (BIE) also process Veteran information in support of claims processing. The purpose of BIE is for other teams to subscribe or consume generated events to take action when an event occurs. BIP Fiduciary Service leverages Benefits Integration Services (BIS), formerly Benefits Gateway Services (BGS), to read data from VA Corporate Database (CRP) for Fiduciary information and passes it to the FAST application for claims determination. Minor/Tenant applications provide, and are responsible for, any data retained in support of their individual mission.

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

The following modules/subsystems are applicable because the system receives, stores, or shares data with them:

- Fraud Prevention RDS Database
- BIP Fiduciary Service
- Benefits Integration Events (BIE)

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

BIP operates in a single region of the VAEC AWS GovCloud, deployed across three Availability Zones (AZs). Both BIP and its Secure Enclave utilize "warm" Disaster Recovery (DR) strategies, with essential data continuously replicated to the DR Region in GovEast. Security and privacy data held by a cloud provider must meet the Privacy Act requirements. Federal agencies must identify and assess the risk to their PII, and to ensure security controls are implemented to provide adequate safeguards. Ensuring that sensitive Veteran data is secure, available, and safe from cyber threats is among the highest priorities of VA OIT and the Enterprise Cloud Solutions Office (ECSO). For that reason, VAEC applications must meet the same rigorous cybersecurity requirements as any other VA IT system. These requirements are defined by the VA Handbook 6500 (Feb. 24, 2021), the VA Directive and Handbook 6517, Risk Management Framework for Cloud Computing Service (Nov. 15, 2016), and the National Institutes of Standards and Technology (NIST).

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

H. What is the citation of the legal authority?

Legal authority to maintain the system is: 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

I. What is the SORN?

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

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

- The SORN does not require amendment or revision.
- The SORN for BIP does cover cloud usage and storage.

4. System Changes

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

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

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

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

Section 1. Characterization of the Information

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

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

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

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

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. It must also match the information provided in question 3.4 of the PTA.

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

- ☒ Name
- ☒ **Full** Social Security Number
- ☐ **Partial** Social Security Number
- ☒ Date of Birth
- ☒ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☒ Personal Fax Number
- ☒ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a Different Individual)
- ☒ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account Numbers
- ☒ Certificate/License Numbers[1]
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☒ Medications
- ☐ Medical Records
- ☒ Race/Ethnicity
- ☒ Tax Identification Number
- ☐ Medical Record Number
- ☒ Sex
- ☐ Integrated Control Number (ICN)
- ☒ Military History/Service Connection
- ☐ Next of Kin
- ☒ Date of Death
- ☐ Business Email Address
- ☐ Electronic Data Interchange Personal Identifier (EDIPI)
- ☒ Other Data Elements (List Below)

Other PII/PHI data elements: Marital Record, Rating Information, Award and Payment Information, Sensitivity Level Information, Relationships to Veteran, Power of Attorney, Military Tour of Duty, Contention Information, Special Issue Information, Claim Information/Decision, VA Username, Exam Information, Document Type, Upload and Metadata, File Number, Veteran Person ID, Claimant Person ID, Benefits Information, DD-214, Verification Status and Participant ID, Home Address, Place of Birth, Biometric Data (e.g., fingerprints, facial recognition), Medical Information, Emergency Contact Records, Educational Records, Employment Information, VA File Number, Veteran and related Dependent and Fiduciary Data, Address of Record, Payment Information, Award Information, Enlistment Date, Insurance Information, Claim Data, Service Number, Active Service Amount, Branch of Service, Pay Grade, Assigned Separation Reason, Service Period, Service-Connected Disabilities and Diagnostics, Reenlisted Indication, Purple Heart or other Military Decoration, Username and Station ID

1.2 List the sources of the information in the system

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

1.2a 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?

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

- BIP does not receive information directly from the individual.
- BIP Minor Applications manage the collection and storage of their own data.

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.

BIP is a platform system that does not contain the ability to or support a business process that requires direct Veteran engagement.

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

BIP does not create information.

1.3 Methods of information collection

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

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

BIP processes Veteran information in support of claims processing on behalf of minor/tenant applications.

BIP stores Veteran and dependent information document data in the FTI Data S3 data store within the FTI Secure Enclave. SFTP - Data feeds from BEP that contain FTI are redirected to this FTI S3 bucket for consumption by BIP FTI Minor Applications via RESTful APIs. Minor/Tenant applications provide, and are responsible for, any data retained in support of their individual mission.

The Fraud Prevention DB is fed by Amazon Data Migration Service (DMS) replicating via Java Database Connectivity (JDBC) connection to the VBA Corporate Database (CRP).

BIP Confluent collects Change Data Capture (CDC) events transmitted via direct Java Database Connectivity (JDBC) connection to BIA BIP Claims Database, VBMS Database, VBA Corporate Database, and VEFS Claim Evidence Database.

BIA Services API provides a Representational State Transfer (REST) Application Programming Interface (API) over Hypertext Transfer Protocol Secure (HTTPS) for Salesforce GovCloud. This API retrieves data from BEP via Simple Object Access Protocol over Mutual Transport Layer Security (mTLS)

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

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

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

BIP does not perform data quality checks. VBA is ultimately responsible for accuracy of data and documents. Minor/Tenant applications are responsible for the quality of any data utilized in support of their individual mission.

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?

N/A

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

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

- VA Compensation, Pension Education, and Vocational Rehabilitation Employment Records -VA SORN 58VA21/22/28 86 FR 61858 *https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf*
- Legal authority to maintain the system is: 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

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: The Secure Enclave stores SPI on Veterans and dependents to support claims processing. If this information were breached or accidentally released to inappropriate parties or the public, it could result in potential personal and/or emotional harm to the friends/relatives of the individuals whose information is contained in the system.

Mitigation: BIP's FTI Secure Enclave implements the Safeguards described in IRS Publication 1075 for protection of FTI. Additionally, the Department of Veterans Affairs is careful to only collect the information necessary to determine eligibility of those Veterans and dependents that file claims. By only collecting the minimum necessary information to process each request, the VA can better protect the individual's information. Records are only released only to authorized VSRs working the claim. The Department of Veterans Affairs applies consistent security guidance to centralize and standardize account management, network access control, database security, vulnerability scanning and remediation.

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.

VBA Veteran Service Representatives (VSR) processing disability and pension claims use Veteran and claim data generated from CDC events to make eligibility, rating, and award determinations for Veterans and dependent benefits. Additionally, VSRs processing pension claims sometimes use documents containing FTI data to make income eligibility determinations for Veteran benefits.

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
First, Middle, and Last Name	Claims Determination	Claims Determination
Social Security Number	Claims Determination	Claims Determination
Date of Birth	Claims Determination	Claims Determination
Personal e-Mail Address	Claims Determination	Claims Determination
Personal Mailing Address	Claims Determination	Claims Determination
Phone Number	Claims Determination	Claims Determination
Contact Numbers	Not used internally	Claims Determination
Tax Identification Numbers	Claims Determination	Claims Determination
Date of Death	Claims Determination	
Marital Record	Claims Determination	
Financial Information	Claims Determination	Claims Determination
Rating Information	Claims Determination	Claims Determination
Award and Payment Information	Claims Determination	Claims Determination
Sensitivity Level Information	Claims Determination	Not used externally
Relationships to Veteran	Claims Determination	Claims Determination
Power of Attorney	Claims Determination	Claims Determination
Military Tour of Duty	Claims Determination	Not used externally
Contention Information	Claims Determination	Not used externally
Special Issue Information	Claims Determination	Not used externally
Claim Information/Decision	Claims Determination	Not used externally
VA Username	Claims Determination	Not used externally
Exam Information	Claims Determination	Not used externally
Military History/Service Connection	Claims Determination	Not used externally
Document Type, Upload and Meta Data	Claims Determination	Not used externally
File Number	Claims Determination	Not used externally
Veteran Person ID	Claims Determination	Not used externally
Claimant Person ID	Claims Determination	Not used externally
Mother's Maiden Name	Claims Determination	Not used externally
Current Medications	Claims Determination	Not used externally
Race/Ethnicity	Claims Determination	Not used externally
Sex	Claims Determination	Not used externally
Benefits Information	Claims Determination	Not used externally
DD-214	Claims Determination	Not used externally
Verification Status and Participant ID	Claims Determination	Not used externally
Home Address	Claims Determination	Not used externally
Place of Birth	Claims Determination	Not used externally

Biometric Data (e.g., fingerprints, facial recognition)	Claims Determination	Not used externally
Medical Information	Claims Determination	Not used externally
Emergency Contact Records	Claims Determination	Not used externally
Educational Records	Claims Determination	Not used externally
Employment Information	Claims Determination	Not used externally
VA File Number	Claims Determination	Not used externally
Veteran and related Dependent and Fiduciary Data	Claims Determination	Not used externally
Address of Record	Claims Determination	Not used externally
Payment Information	Claims Determination	Not used externally
Award Information	Claims Determination	Not used externally
Enlistment Date	Claims Determination	Not used externally
Insurance Information	Claims Determination	Not used externally
Claim Data	Claims Determination	Not used externally
Service Number	Claims Determination	Not used externally
Active Service Amount	Claims Determination	Not used externally
Branch of Service	Claims Determination	Not used externally
Pay Grade	Claims Determination	Not used externally
Assigned Separation Reason	Claims Determination	Not used externally
Service Period	Claims Determination	Not used externally
Service-Connected Disabilities and Diagnostics	Claims Determination	Not used externally
Reenlisted Indication	Claims Determination	Not used externally
Purple Heart or Other Military Decoration	Claims Determination	Not used externally
Username and Station ID	Claims Determination	Not used externally

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

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

BIP does not perform any kind of data analysis or run analytic tasks.

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.

BIP does not create information.

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

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

- BIP protects the confidentiality and integrity of the transmitted information within the system boundary. BIP Platform utilizes Amazon Elastic Block Storage (EBS) and Amazon Simple Storage Service (S3) for platform component storage, including platform operational state from the distributed state model, as well as for log files and log aggregators that could contain Personally Identifiable Information (PII)/Protected Health Information (PHI) from BIP minor applications. Amazon EBS and Amazon S3 provides encryption of the data. Under the management of the BIP System Team, data at rest is encrypted in BIP and while in transit that data is under the governance of VA Enterprise Cloud (VAEC) while both VAEC and BIP share the Transport Layer Security (TLS) portion utilizing TLS 1.2 with weaker cipher suites disabled and TLS 1.3. BIP applications use Secure Socket Layer (SSL) certificates, created by the VA Public Key Infrastructure (PKI) helpdesk.
- FTI data is stored in an isolated S3 bucket and is encrypted at rest using FIPS 140-2 certified AWS Key Management Service (KMS) Customer Managed Key(s) (CMK). The Identity Access Management (IAM) role needed to access the CMK is only given to Government employees. Data to be used by claims processors (VBA end users) is retrieved via a secure proxy solution, the FTI File Repository minor application, deployed to an AWS Elastic Container Service (ECS) cluster running on EC2 instances. These containerized FTI minor application workloads are auto-deployed entities, and contractors are not given access to them unless they are in a maintenance mode where the IAM role with access to the CMK for decryption has been removed.
- Amazon Relational Database Service (RDS) Databases are encrypted at rest using Transparent Data Encryption (TDE). Data in transit between the database and client applications is encrypted using AWS Native Network Encryption (NNE).
- Amazon EBS encrypts volume with a data key using industry-standard AES-256 data encryption. The data key is generated by AWS KMS and then encrypted by AWS KMS with your AWS KMS key prior to being stored with your volume information. All snapshots, and any subsequent volumes created from those snapshots using the same AWS KMS key share the same data key.
- When a new file system is created using the Amazon Elastic File System (EFS) console, encryption at rest is enabled by default. Amazon EFS uses industry-standard AES-256 encryption algorithm to encrypt EFS data and metadata at rest. Amazon EFS integrates with AWS KMS for key management.

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

BIP is an internally hosted platform, meaning that only authorized users can access, and those users must be on the VA network which insulates BIP from any outside/public access. BIP employs a variety of security measures that satisfy controls dictated within the VA 6500 Rev 4 Directive. BIP enforces the flow of information within the system by using several technologies. AWS Virtual Private Clouds (VPCs) are used to separate non-production environments from production environments and security groups to enforce ports, protocols, and services for individual systems within each environment. BIP implements Transport Layer Security (TLS 1.2 with weaker cipher suites disabled and TLS 1.3) encryption adhering to FIPS 140-2 validated mechanisms. Under the management of the BIP System Team, data at rest is encrypted in BIP and while in transit, that data is under the governance of VAEC while both VAEC and BIP share the TLS portion. BIP applications use Secure Socket Layer (SSL) certificates, created by the VA Public Key Infrastructure (PKI) helpdesk.

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

All users, employees, and contractors are required to take VA Privacy and Rules of Behavior, which includes training on how to safeguard PII/PHI.

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?

Access to sensitive data is determined via RBAC (role-based access control) through the following:

- Common Security Services (CSS) – End user access to Minor Application UIs
- VA Identity & Access Management (IAM) – End user access to Minor Application UIs

- RedHat Identity Management System (IdM) – Confluent Kafka events
- VA Okta – Application Container Logs
- VA Active Directory – AWS Console Access

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

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 that all personnel must complete via the VA's Talent Management System 2.0 (TMS). After the user's initial acceptance of the rules, the user must re-affirm their acceptance annually as part of the privacy and security awareness training. Acceptance is obtained via electronic acknowledgement and is tracked through the TMS 2.0 system. Controls and responsibilities are documented within BIPs Access Control (AC) Standard Operating Procedure which is located in BIPs SharePoint folder.

2.4c Does access require manager approval?

Yes, user access requires VA approval from COR/Supervisor/ISO, as well as the BIP PMs, for both general and privileged accounts.

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

- Yes, Automated User account management occurs at multiple levels with respect to the BIP Platform due to the layered architecture and implementation of services upon the platform. BIP currently employs Red Hat IdM and VA Okta to support the management of information system accounts.
- All access to PII data is being logged to centralizing logging and monitoring via AWS OpenSearch.

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

- BIP minor applications/tenant systems manage their application access processes. In the FTI Secure Enclave, access to the PII is determined by authentication and authorization mechanisms implemented in the Veterans Benefits Management System (VBMS) and associated VBMS-managed BIP Minor Applications.
- Administrator accounts on both BIP and FTI Secure Enclave are governed via VA Active Directory/ePAS and requires VA approval from COR/Supervisor, as well as the BIP ISO and/or BIP PMs.

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*

- Date of Birth (DOB)
- Address
- Contact Numbers
- Phone Number
- Financial Information
- Rating Information
- Social Security Number (SSN)
- Award and Payment Information
- Relationships to Veteran
- Power of Attorney
- Tax Identification Numbers
- Mother's maiden name
- Personal Fax Number
- Medications
- Gender
- Date of Death
- Marital Record
- Sensitivity Level Information
- Military Tour of Duty
- Contention Information
- Special Issue Information
- Claim Information/Decision
- VA Username
- Exam Information
- Document Type
- Upload and Meta Data
- File Number
- Veteran Person ID
- Claimant Person ID
- Race/Ethnicity
- Benefits Information
- DD-214
- Username and Station ID

3.2 How long is information retained?

In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please

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

- All data is retained for seven years and is owned by the VA. Recovery Audit System Files: Inputs- destroy/delete source data after data is entered into the master file or database and verified, or when no longer needed to support construction of, or serve as backup to, the master file or database, whichever is later. Prior to decommissioning of system(s), AWS must receive written approval from the VA before destroying any VA provided information. Any data destruction done on behalf of the VA must be in accordance with National Archives and Records Administration (NARA) requirements as outlined in GRS 3.1 and GRS 3.2 (GRS 20).
- Minor/Tenant applications provide, and are responsible for, any data retained in support of their individual mission.

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

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

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

- Retention requirements are governed by the Veterans Benefits Administration (VBA) and National Cemetery Administration (NCA).
- Minor/Tenant applications provide, and are responsible for, any data retained in support of their individual mission.

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

- These records are retained and disposed of in accordance with the General Records Schedule 3.1 and 3.2 (GRS 20), approved by National Archives and Records Administration (NARA) https://www.archives.gov/records-mgmt/grs.html
- Minor/Tenant applications provide, and are responsible for, any data retained in support of their individual mission.

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.

- Electronic media sanitization, when the records are authorized for destruction (or upon system decommission), will be carried out in accordance with VA 6500.1 HB Electronic

Media Sanitization. Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans' Affairs VA Directive 6371, (April 8, 2014), http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=742&FType=2

- Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with the Department of Veterans' Affairs Handbook 6500.1, Electronic Media Sanitization (November 3, 2008), http://www.va.gov/vapubs/viewPublication.asp?Pub_ID=416&FType=2
- Magnetic media is wiped and sent out for destruction per VA Handbook 6500.1. Digital media is shredded or sent out for destruction per VA Handbook 6500.1.
- Additionally, this system follows Field Security Service (FSS) Bulletin #176 dated April 9, 2014 for Media Sanitization Program, SOPs - FSS - All Documents as well as FSS Standard Operating Procedures (SOP) MP-6 Electronic Media Sanitization.

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training, and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

PII stored within BIP's FTI Secure Enclave, Fraud Prevention Database, and Components are not used for research, training or testing.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

Principle of Data Quality and Integrity: The PIA should describe policies and procedures for how PII that is no longer relevant and necessary is purged.

This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk: If information is retained longer than specified, privacy information may be released to unauthorized individuals.

Mitigation: The risk associated with the length of time the data is retained is considered minimal. All data at rest within the BIP security boundary is encrypted in accordance with FIPS 140-2, as well as protected by FedRAMP certified "HIGH" security controls. Use of FedRAMP HIGH controls implemented under the FedRAMP ATO. Collectively, these controls within the BIP security boundary provide maximum protection to all BIP data. BIP only retains the required relevant information relevant as long as necessary to fulfill the specified purpose(s) and in accordance with a National Archives and Records Administration (NARA)-approved record retention schedule.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

PII Mapping of Components

4.1a BIP consists of 8 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 BIP and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

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

Fraud Prevention RDS Database	Yes	Yes	• First, Middle, and Last Name • Date of Birth (DOB) • Address • Phone Number • Financial Information • Rating Information • Social Security Number (SSN) • Award and Payment Information • Relationships and Power of Attorney	Fraud Prevention RDS Database serves as a clone of CRP DB Production that is made available to the Fraud Prevention team so that they can run expensive queries and analysis to detect potential instances of fraud, waste, and abuse.	Amazon RDS uses the industry-standard AES-256 encryption algorithm to encrypt data at rest on the server, leveraging Transparent Data Encryption (TDE). Data in transit between the database and client applications is encrypted using AWS Native Network Encryption (NNE).
BIP Fiduciary Service	Yes	Yes	• First, Middle, and Last Name • Social Security Number (SSN) • Date of Birth (DOB) • Sex • Marital Status • Address • Email Address • Phone Number • User ID	Serves as a passthrough service to FAST application for Claims determination.	JWT tokens to secure endpoints and HTTPS for transmission.

			• Verification Status and Participant ID		
Benefits Integration Events (BIE)	Yes	Yes	• First, Middle, and Last Name • Home Address • Email Address • Phone Number • Social Security Number (SSN) • Date of Birth (DOB) • Place of Birth • Driver's License Number • Biometric Data (e.g. fingerprints, facial recognition) • Financial Account Numbers • Mother's Maiden Name • Race • Sex • Medical Information • Emergency Contact Records • Educational Records • Employment Information • VA File Number	BIE is composed of a multitude of events. Events have a specific focus on an "action" or "event" that has occurred. These events contain PII.	The fields are protected by TLS/SSL encryption during transit and access to data by consumers is whitelisted by role based access controls (RBAC). Access to data at rest is only available to operations members who undergo VA High background investigations.
Benefits Applications Authorization	No	No	N/A	N/A	N/A

Services (BAAZ)					
Machine Learning – Modeling, Analytics, and Training Service (ML-MATS)	No	No	N/A	N/A	N/A
Benefits Innovation Hub (BIH)	No	No	N/A	N/A	N/A
BIP Reference Person (BRP)	No	No	N/A	N/A	N/A
BIP Monitoring System (BMS)	No	No	N/A	N/A	N/A

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

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

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

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

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

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

Data Shared with Internal Organizations

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
Benefits Enterprise Platform (BEP), eMASS ID# 2237	To process Veteran Claims	FTI documents may include Social Security Number, Address, Name and Financial Information, Personally Identifiable Information (PII) including, but not limited to: Veteran and related dependent and Fiduciary data including Name, SSN, Birthdate, Date of Death, Sex, Marital Status and Address of Record	SFTP – Data feeds from VBA users that contain FTI are redirected to this FTI System Simple Object Access Protocol (SOAP) over Mutual Transport Layer Security (mTLS)
VBA Corporate Database (CRP), eMASS ID# 2313	To process Veteran Claims	First, Middle, and Last Name, Date of Birth (DOB), Address, Phone Number, Financial Information, Rating Information, Social Security Number (SSN), Payment Information, Sensitivity Level Information, Award Information, Power of Attorney, Military Tour of Duty, Relationships, Contention Information, Special Issue Information, Claim Information	Change Data Capture (CDC) events transmitted via direct Java Database Connectivity (JDBC) connection to database.
Veterans Benefits Management System (VBMS) Database	To process Veteran Claims	First, Middle and Last Name, Date of Birth (DOB), Address, Phone Number, Financial Information, Rating Information, Social Security Number (SSN), Exam Information, Special Issue Information, Contention Information, Power of Attorney, Military Service, Award Information, Relationships, Document Type, Upload and Meta Data,	Change Data Capture (CDC) events transmitted via direct Java Database Connectivity (JDBC) connection to database.

IT system and/or Program office. Information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List PII/PHI data elements shared/received/transmitted.*	*Describe the method of transmittal*
		Claim Information and Decision, DD-214, Benefits Information	
VEFS Claim Evidence Database	To process Veteran Claims	First, Middle and Last Name, File Number, Social Security Number (SSN), Power of Attorney, Document Meta Data, Veteran Person ID, Claimant Person ID, Date of Death	Change Data capture (CDC) events transmitted via direct Java Database Connectivity (JDBC) connection to database.
BIA BIP Claims Database	To process Veteran Claims	VA Username	Change Data capture (CDC) events transmitted via direct Java Database Connectivity (JDBC) connection to database.
Veterans Benefits Administration (VBA)	To process Veteran Claims	First, Middle and Last Name, Social Security Number (SSN), Data of Birth, Mother's Maiden Name, Personal Mailing Address, Personal e-mail Address, Financial Account Information, Current Medications, Race/Ethnicity, Tax Identification Number, Sex, Military History/Service Connection	Compensation and Pension Record Interchange (CAPRI) Electronic Software Package
VA Salesforce Government Cloud Plus	To process Veteran Claims	Personally Identifiable Information (PII) including, but not limited to: Veteran and related dependent and Fiduciary data including Name, SSN, Date of Birth, Date of Death, Sex, Marital Status and Address of Record	Representational State Transfer (REST) Application Programming Interface (API) over Hypertext Transfer

IT system and/or Program office. Information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List PII/PHI data elements shared/received/transmitted.*	*Describe the method of transmittal*
			Protocol Secure (HTTPS)

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: Sharing of protected Veteran data is necessary to support VA benefits processing/ensure eligible Veterans receive the VA benefits they are entitled however, sharing of any information carries with it a risk of unauthorized disclosure.

Mitigation: BIP mitigates the risk of improperly disclosing protected Veteran data to an unauthorized internal VA entity and/or VA personnel by limiting access only those VA entities and personnel with approved access and clear business purpose/need to know. Additionally, the Veteran provides consent for use of PII data by the completion of benefits forms. The principle of need to know is strictly adhered to. BIP shares information 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 List the external organizations (outside VA) that information shared/received. and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.

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

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

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

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

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

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

Data Shared with External Organizations

List IT System or External Program Office information is shared/received with	***List the purpose of information being shared / received / transmitted***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)***	***List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
Social Security Administration	To process Veteran Claims	Name, Address, Enlistment Date, Date of Death, File Number, Social Security Number, Date of Birth, Insurance Information, Claim Data, Mother's Maiden Name, Service Number, Active Service Amount, Branch of Service, Character of Service, Pay Grade, Assigned Separation Reason, Service Period, Service-Connected Disabilities and Diagnostics, Reenlisted Indication, and Purple Heart or other Military Decoration	National ISA/MOU Record Number: E-5298	Site-to-Site FIPS 140-2 validated VPN tunnel via TCP on ports 443 and 22. Data transferred between SSA and BIP is encrypted over HTTPS or SSH File Transfer Protocol (SFTP) using Transport Layer Security (TLS) 1.2 with weaker

				cipher suites disabled and 1.3 standards. Interface authentication mechanisms are required and could include the use of JavaScript Object Notation (JSON) Web Tokens (JWT), Simple Object Access Protocol (SOAP) Web Security, SSL certificate-based authentication, etc.

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: The VA cannot control what authorized users do with the data they view, after they view it; therefore, it could potentially be shared with entities and individuals without proper permissions to access the data; however, that risk would fall on the application through which the user was accessing that is stored within BIP. Further, there is an established MOU/ISA between BIP and the Social Security Administration (SSA).

Mitigation: All personnel with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually. All users are required to adhere to all information security requirements instituted by the VBA. Information is shared in accordance with VA Handbook 6500. All personnel accessing Veteran's information must first have a successfully adjudicated fingerprint check. This fingerprint check is conducted by the Federal Bureau of Investigation (FBI) Justice Information and criminal history records. Individual users are given access to Veteran's data through the issuance of a user ID and password, and by the use of a Personal Identity Verification (PIV) card. This ensures the identity of the user by requiring two-factor authentication.

Section 6. Notice

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

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

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

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

This is not applicable to BIP as the system does not engage directly with the Veteran or claimant.

6.1b If notice was not provided, explain why.

This is not applicable to BIP as the system does not engage directly with the Veteran or claimant.

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

This is not applicable to BIP as the system does not engage directly with the Veteran or claimant.

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.

This is not applicable to BIP as the systems does not engage directly with the Veteran or claimant

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.

This is not applicable to BIP as the systems does not engage directly with the Veteran or claimant.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Follow the format below:

Privacy Risk: An individual may not receive notice that the BIP exists within the VA.

Mitigation: The VA mitigates this risk by providing Veterans and other beneficiaries with multiple forms of notice of information collection, retention, and processing. The main forms of notice are the Privacy Act statement, System of Record Notice (SORN), and the publishing of this Privacy Impact Assessment.

Section 7. Access, Redress, and Correction

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

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

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

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

- Individuals seeking information regarding access to and contesting of VA records may write, call, or visit the nearest VA regional office. See VA SORN Compensation, Pension, Education and Employment Records-VA, SORN 58VA21/22/2886 FR 61858 (November 08, 2021).

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.

- Individuals seeking information regarding access to and contesting of VA records may write, call, or visit the nearest VA regional office. See VA SORN Compensation, Pension, Education and Employment Records-VA, SORN 58VA21/22/2886 FR 61858 (November 08, 2021).

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

- Individuals seeking information regarding access to and contesting of VA records may write, call, or visit the nearest VA regional office. See VA SORN Compensation, Pension, Education and Employment Records-VA, SORN 58VA21/22/2886 FR 61858 (November 08, 2021).

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.

- Individuals seeking information regarding access to and contesting of VA records may write, call, or visit the nearest VA regional office. See VA SORN Compensation, Pension, Education and Employment Records-VA, SORN 58VA21/22/2886 FR 61858 (November 08, 2021).

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

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: The individual must be provided with the ability to find out whether a project maintains a record relating to them.

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

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

Follow the format below:

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

Mitigation: By publishing this PIA and the applicable SORN, the VA makes the public aware of the unique status of applications and 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 files.

Section 8. Technical Access and Security

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

8.1 The procedures in place to determine which users may access the system, must be documented.

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

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

- BIP minor applications/tenant systems manage their application access processes. In the FTI Secure Enclave, access to the PII is determined by authentication and authorization mechanisms implemented in the Veterans Benefits Management System (VBMS) and associated VBMS-managed BIP Minor Applications.
- Administrator accounts on both BIP and FTI Secure Enclave are governed via VA active directory and requires VA approval from COR/Supervisor, as well as the BIP Operations Manager.

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?

- BIP does not allow external agencies to access BIP owned data.
- BIP minor applications/tenant systems manage their application access processes.

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.

- BIP minor applications/tenant systems manage their application access processes. In the FTI Secure Enclave, access to the PII is determined by authentication and authorization mechanisms implemented in the Veterans Benefits Management System (VBMS) and associated VBMS-managed BIP Minor Applications.
- Administrator accounts on both BIP and FTI Secure Enclave are governed via VA active directory and requires VA approval from COR/Supervisor, as well as the BIP Operations Manager.

- Only System Administrators are granted administrative roles. Permissions granted on a least privileged basis as determined by the VA COR and the BIP Operations Manager.
- Role Based Access Controls (RBAC) are in place and govern general user/administrator access.

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

How frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.

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

Yes

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

- VA Contractors have been tasked with operation and managements of the Benefits Integration Platform (BIP) in production. Such tasking necessitates access to the PII. Contractors do not have access to FTI secure enclave data.

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

- VA Contractors will design and maintain the system. Contractors do not have access to FTI secure enclave data.

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.

- Contractors supporting BIP must complete annual the following training via the VA's Talent Management System:
    - VA Privacy and Information Security Awareness and Rules of Behavior (PISA) – annually required training
    - Privacy & HIPAA – annually required training
    - Information Security Role-Based Training for IT Specialists (WBT) – one-time training

- Introduction to the One-VA Technical Reference Model (TRM) – one-time training

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

8.4a If completed, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 19-Mar-2025
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* 30-Jun-2024
5. *The Authorization Termination Date:* 27-Jun-2026
6. *The Risk Review Completion Date:* 30-Jun-2024
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 not completed or In Process, provide your ***Initial Operating Capability (IOC) date.***

N/A

Section 9 – Technology Usage

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

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

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

- BIP operates as a Platform as a Service (PaaS) model and is hosted in the VAEC AWS GovCloud, FedRAMP Package ID F1603047866.

9.2 Does the contract with the Hosting Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). ***(Refer to question 3.3.1 of the PTA)*** *This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

The VA maintains ownership of the data, and selects which services can process, store, and host data. The CSP does not access or use the data for any purpose without agreement from the VA. VAEC determines where the data will be stored, including the type of storage and geographic region of that storage. VAEC manages access to its data, and access to services and resources through users, groups, permissions, and credentials that are internally controlled. VAEC chooses the secured state of the data. The CSP provides encryption features that protect data in transit and at rest and provides VAEC with the option to manage their encryption keys. VAEC AWS Enterprise Cloud Capacity Contract - NNG15SD22B VA118-17-F-2284.

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.

The CSPs automatically collect metrics, such as offering usage, occurrences of technical errors, diagnostic reports, settings preferences, backup information, API calls, and other logs. VAEC is the owner of its data (customer data). The CSP does not use customer data and has anonymized metrics to help them measure, support, and improve their services. The CSP has ownership of these anonymized metrics.

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.

Each application in the VAEC is responsible for their data. For all cloud deployment types, the customer owns their data and identities. The customer is responsible for protecting the security of their data and identities, on-premises resources, and the cloud components they control (which varies by service type). This is the Shared Responsibility Model for Security in the Cloud.

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).

BIP personnel utilize GitHub Copilot, an AI-powered coding assistant aimed at automating tasks and increasing efficiency. Users cannot input PII/PHI information into GitHub Copilot.

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.

MARVIS HARVEY

Digitally signed by MARVIS HARVEY
Date: 2025.06.30 13:19:51 -05'00'

Privacy Officer, Marvis Harvey

JOSEPH FACCIOLLI

Digitally signed by JOSEPH FACCIOLLI
Date: 2025.06.30 11:55:29 -04'00'

Information System Security Officer, Joseph Facciolli

TUSHAR DODE

Digitally signed by TUSHAR DODE
Date: 2025.06.30 13:10:39 -04'00'

Information System Owner, Tushar Dode

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).

This is not applicable to BIP as the systems does not engage directly with the Veteran or claimant.

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

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

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

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

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

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