Privacy Impact Assessment for the VA IT System called:

Federal Tax Information File Repository (FFR)

Veterans Benefits Administration (VBA)

Office of Business Integration (OBI)

eMASS ID # 2057

Date PIA submitted for review:

12/10/2024

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)	Joseph Facciolli	Joseph.Facciolli@va.gov	212-842-2999x2012
Information System Owner	Christina Lawyer	Christina.Lawyer@va.gov	518-210-0581

Abstract

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

The Federal Tax Information (FTI) File Repository (FFR) is hosted on the Benefits Integration Platform (BIP) and contains Federal Tax Information provided by the Internal Revenue Service (IRS) to the VA for use in determining award eligibility for claimants. The FFR is a tenant of the FTI Secure Enclave environment that implements the safeguards necessary for housing FTI in the cloud. FTI Simple Object Access Protocol (SOAP) will ingest the documents and the FFR will contain the FTI documents. The system, in use of the data, will be used to decommission several legacy Veterans Benefits Administration (VBA) systems and enable the Pension Automation system to implement an Application Programming Interface (API) to make income eligibility determinations. The FFR application is a tenant of the BIP Secure Enclave environment which has been approved by the Internal Revenue Service (IRS) Office of Safeguards (memo FD698-FED-AWS GovCloud-L-031020) as adequately implementing the safeguards outlined in IRS Publication 1075 and in accordance with Internal Revenue Code §6103(p)(4).

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?

Federal Tax Information (FTI) File Repository (FFR) is under the authority of the Veterans Benefits Administration (VBA) Program office in the Office of Information Technology (OIT). This system is a tenant of the BIP Secure Enclave environment that implements the safeguards necessary for housing FTI in the cloud. The FFR provides a safeguarded repository to store FTI data to be used in claims processing.

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.

VA Owned and VA Operated

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?

The FFR stores roughly 300,000 eligible Veteran's information. The FTI File Repository will contain FTI data to support the pension claims process.

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?

- Name: Used to identify the claimant or Veteran
- Social Security Number: May be supplied by the IRS to uniquely identify the claimant or Veteran.
- Date of Birth: May be supplied by the IRS to uniquely identify the claimant or Veteran
- Personal Mailing Address: May be included in Tax Return information provided by IRS. Also, will be included in FTI letters to the claimant or Veteran
- Personal Phone Number: May be included in Tax Return information provided by IRS
- Personal Fax Number: May be included in Tax Return information provided by IRS
- Personal Email Address: May be included in Tax Return information provided by IRS
- Emergency Contact Information (Name, Phone Number, etc. of a different individual): May be included in Tax Return information provided by IRS
- Financial Account Information: Supplied by the IRS to make income eligibility determinations within the Pension claims process
- Tax Identification Number: May be supplied by the IRS to uniquely identify the claimant or Veteran
- Benefit Information: May be supplied by the IRS for identification purposes
- Relationship to Veteran: May be supplied by the IRS for identification purposes

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

FTI File Repository is hosted on Benefits Integration Platform (BIP). BIP provides a container-based application platform in VAEC AWS in which VA benefits, appeals, and

memorial (BAM) and Federal Tax Information (FTI) applications can be hosted. The platform leverages Kubernetes 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 is locked down to only allow container images to be mirrored between registries in each VPC. BIP also leverages a suite of TRM approved COTS tools (e.g. Jenkins, SonarQube, 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 controls necessary for applications hosted on the platform. Minor applications and application programming interfaces (APIs) are hosted on BIP Assessing on VAEC AWS.

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

No, the modules/subsystems are applicable even if information is not shared.

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?

FTI File Repository resides in a virtual environment within the Veterans Administration Enterprise Cloud (VAEC) which is hosted within Amazon Web Services (AWS) – this environment and access control ensures accessibility and provides data integrity and consistency across all sites used to access the application through the VA network.

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

H. What is the citation of the legal authority?

• 5 U.S.C. § 552a, Freedom of Information Act of 1996, As Amended By Public Law No. 104--- 231, 110 Stat. 3048
• 5 U.S.C. § 552a, Privacy Act of 1974, As Amended
• Public Law 100---503, Computer Matching and Privacy Act of 1988
• Privacy Act of 1974; U.S Code title 5 USC section 301 title 38 section 1705,1717, 2306-2308 & Title38, US Code section 7301 (a) and Executive Order9397
• OMB Circular A---130, Management of Federal Information Resources, 1996
• OMB Memo M---03---22, OMB Guidance for Implementing the Privacy Provisions
• OMB Memo M---07---16, Safeguarding Against and Responding to the Breach of PII
• The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
• State Privacy Laws
• The legal authority is 38 U.S.C 7601-7604 and U.S.C 7681-7683 and Executive Order 9397
• System of Record Notice (SORN) 58VA21/22/28 (November 8, 2021) Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA

https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

I. What is the SORN?

58VA21 - Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA"
https://www.oprm.va.gov/docs/SORN/Current_SORN_List_01_2 7_2023.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.

No amendments or revisions to the SORN are required. The SORN covers cloud usage (VAEC).

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
- ☐ Gender/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:
Benefit Information
Relation to Veteran

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?

BIP Minor Applications manage their own information sources of data. In the current process FTI documents are captured at 3 Regional offices, Milwaukee, Philadelphia, and St. Paul. In the Secure Enclave, Veteran Service Representatives (VSRs) processing pension claims sometimes use FTI data to make income eligibility determinations for Veteran benefits.

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

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

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.

In the Secure Enclave, Veteran Service Representatives (VSRs) processing pension claims sometimes use FTI data to make income eligibility determinations for Veteran benefits.

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

The system 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 Minor Applications manage their information collections processes. In the FFR, FTI information is provided directly from IRS or through a subsidiary at the Social Security Administration (SSA) and is accessible in the VETSNET Share application. From Share, users will upload documents to the FFR.

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?

Information is not collected on a form.

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 Minor Applications manage their data validation processes. In the FFR, standard operating procedures (SOPs) are in place at the Pension Centers to perform quality control on data related to each claim.

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?

The claim level quality control checks are performed before award, and random claim samples are also collected monthly for further review by quality control specialists.

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

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

The System of Record Notice (SORN) "VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA" 58VA21/22/28 (November 8, 2021). This SORN can be found online at https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf 5 U.S.C. § 552a, Freedom of Information Act of 1996, As Amended By Public Law No. 104---231, 110 Stat. 3048 5 U.S.C. § 552a, Privacy Act of 1974, As Amended IRS memo FD698-FED-AWS GovCloud-L-031020. A current record of VA Sorns can be found at https://www.oprm.va.gov/docs/Current_SORN_List_10_19_2021.pdf.
For the Secure Enclave, legal authority for Federal Tax Information, to include identity information, be shared between Department of the Treasury/IRS and VA is codified in Internal Revenue Code §6103(l)(7), with identity information codified in §6103(b)(6). The ISA/MOU governing the information exchange between IRS and VA is codified in DART 52.
As for the Veteran eFolder in Virtual VA (VVA) within which FTI documents will be available, the Secretary of Veterans Affairs established guidelines pursuant to the authorities in and requirements of Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources," and the authorities contained under Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of Resources 31with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency Agreements," also known as the "Economy Act." These guidelines assist in the implementation of these statutes.

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: The 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 Pension 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.

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	Used to identify the claimant or Veteran	Not used
Social Security Number	May be supplied by the IRS to uniquely identify the claimant or Veteran	Not used
Date of Birth	May be supplied by the IRS to uniquely identify the claimant or Veteran	Not used
Personal Mailing Address	May be included in Tax Return information provided by IRS. Also, will be included in FTI letters to the claimant or Veteran	Not used

Personal Phone Number	May be included in Tax Return information provided by IRS	Not used
Personal Fax Number	May be included in Tax Return information provided by IRS	Not used
Personal Email Address	May be included in Tax Return information provided by IRS	Not used
Emergency Contact Information (Name, Phone Number, etc. of a different individual)	May be included in Tax Return information provided by IRS	Not used
Financial Account Information	Supplied by the IRS to make income eligibility determinations within the Pension claims process	Not used
Tax Identification Number	May be supplied by the IRS to uniquely identify the claimant or Veteran	Not used
Benefit Information	May be supplied by the IRS for identification purposes	Not used
Relationship to Veteran	May be supplied by the IRS for identification purposes	Not used

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?

FFR does not perform any kind of data analysis or run analytic task.

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.

FFR does not create or make available new or previously unutilized 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?

Secure Socket Layer (SSL)/Transport Layer Security (TLS) encryption are in place to protect data in transit and at rest.

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

Data is hosted in Amazon Web Services (AWS) and is encrypted both in transit and at rest via SSL/TLS.

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

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

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.

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

Principle of Transparency: Is the PIA and SORN, if applicable, clear about the uses of the information?

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

2.4a How is access to the PII determined?

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

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

Yes, criteria, procedures, controls, and responsibilities regarding access to this system are documented in various sites which are but not limited to TMS, GRC tool, and SharePoint sites.

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 as identified in eMASS?

All employees with access to Veteran's information are required to complete the mandatory VA Privacy and Information Security Awareness training and Rules of Behavior annually. Disciplinary actions, depending on the severity of the offense, include counseling, loss of access, suspension and possibly termination.

VBA end users of the system must take annual FTI awareness and protection training as outlined in IRS Publication 1075. This training must be completed via the VA's Talent Management System 2.0 (TMS) and compliance is tracked through the TMS 2.0 system. Section3. Retention of Information.

Individual users are given access to Veteran's data through the issuance of a user ID and password and using a Personal Identity Verification (PIV) card. This ensures the identity of the user by requiring two-factor authentication. The user's ID limits the access to only the information required to enable the user to complete their job.

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*

- Name
- Social Security Number
- Date of Birth

- Personal Mailing Address
- Personal Phone Number
- Personal Fax Number
- Personal Email Address
- Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- Financial Account Information
- Tax Identification Number
- Benefit Information
- Relationship to Veteran

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.

Data is maintained in accordance with VA data retention policies. FTI File Repository information retention requirements are governed by the Virtual VA (VVA) system from which FTI documents are accessed. The VVA PIA is maintained by the VVA PM. Relevant excerpt from the VVA PIA: Currently the retention period on documents is set to "0": documents never get deleted. This is because requirements were structured to adhere to the paper requirements and for Virtual VA to become of a system of record. 74 FR 29275 published June 19, 2009. http://edocket.access.gpo.gov/2009/pdf/E9-14302.pdf

Virtual VA (VVA) is hosted at Milwaukee and St. Paul Regional Offices and the Philadelphia Information Technology Center (PITC). The response below explains how long each data center retains information:

- PHILADELPHIA: Regarding VVA Scanning Paper Dispositions, the Philadelphia PMC completes the following process after documents are scanned and verified in VVA/LCM/VBMS:
    - If the scanned document is an original received by a claimant, the physical document is mailed back to the claimant (i.e. original copy of a DD-214, original Marriage or Death Certificate, or other types of original discharge or personal/family paperwork).
    - If the document is FTI related, the physical copies are logged and maintained in secured cabinets per VBA FTI guidelines.
    - All other physical paperwork is logged and prepared for shredding based on the guideline provided under VBA 6300. Under this guidance, paperwork is recorded taken to the Regional Office Records Management Officer for proper disposal.
- ST. PAUL: We hold the letters for 90 days after they have been verified in the system, the letters are held in a locked file cabinet then are sent to the records management officer and they are destroyed in a special shredder used only for FTI.

- MILWAUKEE: In regard to VVA Scanning Paper Dispositions, the Milwaukee PMC completes the following process after documents are scanned and verified in VVA/LCM/VBMS:
    - If the scanned document is an original received by a claimant, the physical document is mailed back to the claimant (i.e. original copy of a DD-214, original Marriage or Death Certificate, or other types of original discharge or personal/family paperwork).
    - If the document is FTI related, the physical copies are logged and maintained in secured cabinets per VBA FTI guidelines (IRS Publication 1075).
    - All other physical paperwork is logged and prepared for shredding based on the guidelines provided under M21-1V.iv.2.5 and VBA 6300. Under this guidance, paperwork is recorded and taken to the Regional Office Records Management Officer for proper disposal.

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

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

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

Yes.

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

VBA Records Management, Records Control Schedule VB-1, Part 1, Section VII as authorized by NARA https://www.benefits.va.gov/WARMS/docs/regs/RCS_I.doc

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.

All paper documentation that is not the property of VA (e.g., DoD-owned documentation) is currently stored by VA after scanning, pending a policy determination as to its final disposition. All documentation being held pursuant to active litigation is held in its native format during the pendency of the litigation. All VBMS eFolders are stored on a secure VA server, pending permanent transfer to NARA where they will be maintained as historical records. Once an electronic record has been transferred into NARA custody, the record will be fully purged and deleted from the VA system in accordance with governing records control schedules using commercial off the shelf (COTS) software designed for the purpose. Once purged, the record will be unavailable on the VA system, and will only be accessible through NARA.

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 VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction. https://www.va.gov/vapubs/search_action.cfm?dType=1

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 retained by the FTI File Repository is 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: As described herein, support systems retain information until that work in progress is completed and data is committed to master systems and records. The master systems retain data on a permanent basis (beyond the actual death of the Veteran). If a master system is to be

deactivated, critical information is migrated to the new system and the old system along with associated data is archived according to the application disposition worksheet. As such, SPI, PII or PHI may be held for long after the original record was required to be disposed. This extension of retention periods increases the risk that SPI may be breached or otherwise put at risk.

Mitigation: User access is not provided by VVA but by the ePAS process. The following are true of all VA information system users:

- All employees with access to Veteran's information are required to complete the mandatory VA Privacy and Information Security Awareness training and Rules of Behavior annually.
- Disciplinary actions, depending on the severity of the offense, include counseling, loss of access, suspension and possibly termination.
- Individual users are given access to Veteran's data through the issuance of a user ID and password and using a Personal Identity Verification (PIV) card. This ensures the identity of the user by requiring two-factor authentication. The user's ID limits the access to only the information required to enable the user to complete their job. FFR does not create, adjust, or make documents in any way, but is simply a repository for other systems. If a document is submitted to VVA as redacted, it is input as redacted.

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 **FTI File Repository** consists of **two** 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 **FTI File Repository** 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)	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

etc.) that contains PII/PHI					
Receive VirtualVA (one time migration)	Yes	Yes	FTI documents may include social security number, address, name, and financial information	Eligibility determinations within the claims processing lifecycle.	FFR will implement the safeguards necessary for housing Federal Tax Information in the VAEC AWS GovCloud. Secure Socket Layer (SSL)/Transport Layer Security (TLS) encryption are in place to protect data in transit and at rest.
Share VBMS (User interface)	Yes	Yes	FTI documents may include social security number, address, name, and financial information	Eligibility determinations within the claims processing lifecycle.	FFR will implement the safeguards necessary for housing Federal Tax Information in the VAEC AWS GovCloud. Secure Socket Layer (SSL)/Transport Layer Security (TLS) encryption are in place to protect data in transit and at rest.

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***
VirtualVA	The Virtual VA previously housed the FTI documents. FFR now ingests FTI documents and the metadata from Virtual VA	FTI documents may include Social Security Number, address, name and financial information.	Encrypted SOAP transfer
Veterans Benefits Management Systems (VBMS) Cloud Assessing	FFR implements the safeguards necessary for housing FTI in the cloud. The FFR provides a safeguarded repository to store FTI data to be used in claims processing.	FTI documents may include Social Security Number, address, name and financial information.	Secure iframe temporary file access that requires authentication

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: The sharing of data between VA systems is necessary to support the goals and purpose of the system. However, there is a risk that the data could be shared with an inappropriate VA organization which would potentially impact privacy.

Mitigation: All employees/contractors with access to Veterans' information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually. Information is shared in accordance with VA Handbook 6500. The principle of need-to-know is strictly adhered to by program office. Only personnel with a clear business purpose are allowed access to the system and the information contained within. This action adheres to the

idea of least privilege and need to know found in the VA 6500 Handbook. Access to the system requires a VA issued identity assertion.

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***	***List the method of transmission and the measures in place to secure data***

			be more than one)	
N/A	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

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

Follow the format below:

Privacy Risk: Not applicable, as there is no sharing of information outside of VBA or VA with external parties.

Mitigation: Not applicable, as there is no sharing of information outside of VBA or VA with external parties.

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.

VA gathers or creates these records in order to enable it to administer statutory benefits programs to Veterans, Service Members, Reservists, and their spouses, surviving spouses, and dependents, who file claims for a wide variety of Federal Veteran's benefits administered by VA. See the statutory provisions cited in ''Authority for maintenance of the system". This notice is provided by the SORN for better understanding to the reader.
The System of Record Notice (SORN) as listed in the Federal Register:
58VA21/22/28, *Compensation, Pension, Education, and Rehabilitation Records- VA*
https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

6.1b If notice was not provided, explain why.

No notice is provided to an individual. FFR does not collect information directly from the Veteran but instead data being stored is from the source applications listed in section 1.2 of this PIA. The source systems collecting the information would provide the notice. The System of Record Notice as listed in the Federal Register: 58VA21/22/28, *Compensation, Pension, Education, and Rehabilitation Records- VA* https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf indicates all purposes of use and records categories stored in the FFR system.

When Veterans apply for benefits, The Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected information to individuals applying for benefits. A signed statement acknowledging that the individual read and understood the NOPP.
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

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

The Department of Veterans Affairs provides public notice that the system exists in two ways:

1. The System of Record Notice (SORN) as listed in the Federal Register: 58VA21/22/28, *Compensation, Pension, Education, and Rehabilitation Records- VA*
   https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf
2. This Privacy Impact Assessment (PIA) also serves as notice of the Enterprise Data Warehouse (EDW). As required by the eGovernment Act of 2002, Pub.L. 107–347§208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA]under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."
   https://department.va.gov/privacy/privacy-impact-assessments/

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.

Not applicable. No notice is provided to an individual. Individuals do not have the opportunity and right to decline to provide information. There may be notice provided to the veteran or

claimant outside of FFR when Federal Tax Information is requested. So veterans/claimant may have the right to consent or decline, but that is out of the scope of the FFR functionality. FFR is only meant to provide storage for Federal Tax Information data needed by Veterans Benefit Administration users to support claims processing.

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.

Not applicable. Individuals do not have the right to consent to particular uses of information. No notice is provided to an individual. There may be notice provided to the veteran or claimant outside of FFR when Federal Tax Information is requested. So veterans/claimant may have the right to consent or decline, but that is out of the scope of the FFR functionality. FFR is only meant to provide storage for Federal Tax Information data needed by Veterans Benefit Administration users to support claims processing.

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: Not applicable. As an application, FFR does not provide notice to the individual. FFR's purpose is to provide storage for Federal Tax Information data needed by Veterans Benefit Administration users to support claims processing. Any notice to the veteran or claimant about use of their data would likely come from another part of the claims process**.**

Mitigation: Not applicable. As an application, FFR does not provide notice to the individual. FFR's purpose is to provide storage for Federal Tax Information data needed by Veterans Benefit

Administration users to support claims processing. Any notice to the veteran or claimant about use of their data would likely come from another part of the claims process.

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.***

Procedures are outlined in The System of Record Notice (SORN) "VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records –VA" 58VA21/22/28 (November 8, 2021). This SORN can be found online at https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

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

The system is not exempt from the Privacy Act.

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?

The system is a privacy act system, as such any individual who wishes to determine whether a record is being maintained under his or her name in FFR or wishes to determine the contents of such records, should submit a written request or apply in person to the VA facility where the records are located. For a directory of VA facilities and phone numbers by region, see https://www.benefits.va.gov/benefits/offices.asp

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

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

Documents that are stored in FFR have already been established. Inaccurate or erroneous information cannot be applied to these documents.

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

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

Individuals are not notified as the FFR application only retrieves and stores Federal Tax Information (FTI) data needed by Veterans Benefit Administration (VBA) users to support claims processing documents and cannot modify information contained in the stored documents.

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.

An individual seeking information regarding access to and contesting of VA records may write, call or visit the nearest VA regional office. Address locations are listed in VA Appendix 1, as directed in the System of Record Notice (SORN) "VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA" 58VA21/22/28 (November 28, 2021). This SORN can be found online at: https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. ***For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.*** *(Work with your 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: No access, redress, and correction policies and procedures exist in the scope of the FFR application. There may be the ability to redress or correct the data that is passed through FFR through a formal process in another application, but the application itself does not have a process. Individuals may seek to access or redress their records held by the VA Office and a risk exists that their claim will not be processed correctly.

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

Section 8. Technical Access and Security

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

Access is requested per VA 6500 policies utilizing Electronic Permission Access System (ePAS). Users submit access requests based on need to know and job duties. Supervisor, Information System Owner (ISO) and Office of Information and Technology (OIT) approval must be obtained prior to access being granted. These requests are submitted for VA employees, contractors and all outside agency requests and are processed through the appropriate approval processes. Once access is granted, individuals can log into the system(s) through dual authentication, i.e., a PIV card with a complex password combination (two-factor authentication is enforced). Once inside the system, individuals are authorized to access information on a need-to-know basis.

OIT documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and retains individual training records for 7 years. This documentation and monitoring are performed by the VA's Talent Management System (TMS), the System Owner will then need to review and

approve access to 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?

Only VA Employees and Contractors have access to the system. Users from outside the VA do not have access to the system.

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.

There are End-User, Admin, and Read-Only roles for this system. Per VA Directive and Handbook 6330, every 5 years the OIT develops, disseminates, and reviews/updates a formal, documented policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; along with formal, documented procedures to facilitate the implementation of the control policy and associated controls.

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?

There is a Benefits Integrated Platform (BIP) NDA in place. It covers all personnel working on FFR. The FFR development team is comprised of VA personnel and contractors. Contracts are reviewed annually by the Contracting Officer's Representative (COR).VA OIT provides basic security awareness training to all information system users (including managers, senior executives, and contractors) of VA information systems, or VA sensitive information as part of initial training for new users, when required by system changes, and annually thereafter.

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

A contractor team will support the FFR application, but safeguards are in place to prevent contractor access to Federal Tax Information within FFR in accordance with IRC §6103(p)(4) restrictions. These safeguards were certified by IRS as acceptable in memo FD698-FED-AWS GovCloud-L-031020 and will be audited by IRS during the VA's normal triannual FTI audit. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of Behavior training via the VA's Talent Management System (TMS).

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

Contractors will have access to design and maintenance of applications that utilize FFR.

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

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

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training 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 acknowledgment and is tracked through the TMS 2.0 system.

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:* 10/9/2024
3. *The Authorization Status:* Approved
4. *The Authorization Date:* 12/5/2023
5. *The Authorization Termination Date:* 12/5/2026
6. *The Risk Review Completion Date:* 9/10/2024
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

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

N/A

Section 9 – Technology Usage

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

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

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

Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties. ***(Refer to question 1.8 of the PTA)***

Yes, the system is a Software as a Service (SaaS) hosted on Benefits Integration Platform (BIP) which is hosted in the VA Enterprise Cloud (VAEC).

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 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).

Not Applicable. FFR does not use Robotics Process Automation.

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.

LAKISHA WRIGHT

Digitally signed by LAKISHA WRIGHT
Date: 2024.12.31 09:45:29 -05'00'

Privacy Officer, Lakisha Wright

JOSEPH FACCIOLLI

Digitally signed by JOSEPH FACCIOLLI
Date: 2024.12.31 11:16:37 -05'00'

Information System Security Officer, Joseph Facciolli

CHRISTINA LAWYER

Digitally signed by CHRISTINA LAWYER
Date: 2025.01.02 07:02:19 -05'00'

Information System Owner, Christina Lawyer

APPENDIX A-6.1

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

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)