Privacy Impact Assessment for the VA IT System called:

Salesforce: Fiduciary Accounting Submission Tool (FAST)

Pension and Fiduciary (P&F) Service

Veterans Benefits Administration

eMASS ID # 1944

Date PIA submitted for review:

10/17/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Dontrell Wiggins	Dontrell.Wiggins@va.gov	505-353-0275
Information System Security Officer (ISSO)	James Boring	James.Boring@va.gov	215-842-2000, Ext 4613
Information System Owner	Michael Domanski	Michael.Domanski@va.gov	727-595-7291

Abstract

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

Salesforce - Fiduciary Accounting Submission Tool (SF-FAST) is a community portal where public fiduciaries will be able to submit accountings (and attached documents) electronically to Pension & Fiduciary Hubs for review and approval in a form of Case Management.

Overview

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

1 General Description

A. What is the IT system name and the name of the program office that owns the IT system?
Salesforce - Fiduciary Accountings Submission Tool (SF-FAST) is run on the Salesforce Government Cloud. SF-FAST is owned by Pension and Fiduciary Service.

B. What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?
VA and court appointed Fiduciaries, approximately 174,000, require a portal to electronically submit information and documentation to Fiduciary Hubs which are necessary for the oversight of VA beneficiaries. The typically affected individuals range from Veterans, their dependents, or even members of the public, namely fiduciaries. The module would reduce fax/mail correspondence and entry errors while improving timeliness and increasing communication between the VA and Fiduciaries. The module will provide walkthroughs and guidance to Fiduciaries to simplify the process.

C. Who is the owner or control of the IT system or project?
SF-FAST is run on the Salesforce Government Cloud. SF-FAST is owned by Pension and Fiduciary Service.

2. Information Collection and Sharing

D. What is the expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual?
This system services nationwide and not a regional system. SSNs will be collected for the Veteran/Beneficiary as part of documenting the VA File Number which all likelihood is also the SSN to personally identify that individual. The Privacy Act of 1974, US Code 552a is the legal authority to collect this information.

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

Both internally and externally, SF-FAST currently connects, receives, and shares Personally Identifiable Information (PII) with other internal organizations, IT Systems, websites, or organizations.

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

The method for data sharing is required to provide excellence in service to Veterans, dependents, and members of the public. The initial method of data sharing for SF-FAST is information input by VA employees and Fiduciaries.

Additionally, SF-FAST integrates with Benefit Gateway Service (BGS), Master Patient Index (MPI), and Veterans Benefits Management System - Fiduciary (VBMS-FID). VBMS-FID receives data from SF-FAST to enhance the Fiduciary oversight process. The VBMS tool enables the Fiduciary Program to expedite Veteran qualifications, appointments of fiduciaries, and release withheld VA funds to beneficiaries. Without integrations, authorized VBMS-FID users must manually transcribe data contained in FAST Accounting Records to VBMS-FID Accounting Audit Tool (AAT) for auditing purposes. This integration allows for seamless dataflow of shared files containing PII to eliminate the need for manually downloading, converting, and uploading PDFs to VBMS-FID for information sharing between the two systems.

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

The cloud service provider for SF-FAST is Salesforce Government Cloud Plus - Enterprise (SFGCP -E) hosted on AWS Government Cloud.

In order to gain access to SF-FAST, users must use the Single Sign On (SSO) service using a Personal Identification Verification (PIV) card and associated credentials.

3. Legal Authority and SORN

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

The SF-FAST module is covered under 58VA21/22/28 86 FR 61858, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA. The Privacy Act of 1974 (5 U.S.C. 552a(e)(4)), is the legal authority to collect the information listed in question 1.1. The authority for maintenance of the system is Section 501(a), (b), and chapter 55 of Title 38, United States Code.

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

SF-FAST is covered by SORN#: 58VA21/22/28 86 FR 61858, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, Citation: 78 FR 12423. The aforementioned SORN is located at Federal Register Hyperlink 58VA21/22/28 86 FR 61858. The System Title is Beneficiary Fiduciary Field System (BFFS)-VA.

The SORN is in the process of being modified to include 2 data elements: (1) ICN (Integrated Control Number) and (2) PID (Patient Identifier).

4. System Changes

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

Business processes for Fiduciaries will be enhanced to support automated data sharing between SF-FAST and Veterans Benefits Management System - Fiduciary (VBMS-FID). Instead of manually transcribing SF-FAST accountings into VBMS-FID, fiduciaries will be able to electronically share files containing PII to eliminate the need for manually downloading, converting, and uploading PDFs to VBMS-FID for information sharing between the two systems.

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

SF-FAST will be enhanced to include an integration with VBMS-FID that will utilize a Salesforce REST Apex class integration which allows VBMS to pull data through Digital Transformation Center (DTC) Integration Platform (DIP) middleware. Additionally, DIP middle layer is used to convert fiduciary documents housed in FAST to .pdf prior to the files being transferred via the Claim Evidence API.

Section 1. Characterization of the Information

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

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

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

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

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

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

☒ Name ☒ Social Security Number ☒ Date of Birth
☐ Mother's Maiden Name

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

Other PII/PHI data elements: The "Other Unique" item above is checked to indicate the Business Address, Business Email Address, Business Phone Number, VA File Number, Claim Number, Bank Account Number, and Patient Identifier (PID) are collected, processed, or retained by SF-FAST. SF-FAST does not restrict written comments and acknowledges that those comments may include personal information (bank account numbers) about the Veteran, dependents, or fiduciaries (members of the public). The comments are not released or shared outside of SF-FAST.

PII Mapping of Components (Servers/Database)

SF-FAST consists of two key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by SF-FAST and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that	**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**

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

contains PII/PHI					
SF-FAST	Yes	Yes	VA File #, SSN, Name, Personal/Business Address, Personal/Business Email Address, Personal/Business Phone, Integrated Control Number (ICN), Claim Number, Date of Birth (DOB), Financial Information/Documentation, Bank Account Numbers, PID (patient identifier)	To identify Veterans and to document accountings submissions	Use of SSO for access to the system by internal VA users and ID.me for external user verification; the fields containing PII in Salesforce are encrypted
Claim Evidence Application Programming Interface (API)	Yes	Yes	Veteran Name, SSN, VA File #, PID (patient identifier)	To share data with Veterans Benefits Management System – Fiduciary (VBMS-FID)	The fields containing PII in Salesforce are encrypted

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

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

As part of the intake of information, the public end user, VA employee, or system submitting/transmitting the information provides the name, address, phone number, mailing address, SSN or VA File #, and/or the Financial Account Information. This information is needed to properly identify the Veteran and Fiduciary.

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.

Information is not obtained from other sources other than the Fiduciaries.

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

System uses the integral Salesforce Dashboard to display aggregate data from SF-FAST data collection. No external data is used or collected.

1.3 How is the information collected?

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

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

The information is collected electronically through the SF-FAST module in the Salesforce cloud. The public end user accesses a Salesforce community portal hosted on VA.gov to enter the necessary information.

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?

SF-FAST populates the 21P-4706b and 21P-4703

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

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

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

No information is collected from SF-FAST; therefore, no information needs to be checked for accuracy.

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?

Each financial accounting submission to SF-FAST is addressed by a VBA employee. The accuracy of the information is checked through the working of the fiduciary accounting review by using the information to access other VA established Office of Information Technology (OIT) systems of record.

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

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in

addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect

The SF-FAST module is covered under 58VA21/22/28 86 FR 61858, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA. The Privacy Act of 1974 (5 U.S.C. 552a(e)(4)), is the legal authority to collect the information listed in question 1.1. The authority for maintenance of the system is Section 501(a), (b), and chapter 55 of Title 38, United States Code.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: The risk is similar with any other systems that if the wrong person were to have access to the information, it could be used to obtain financial resources and negatively impact beneficiaries' lives.

Mitigation: The Salesforce Government Cloud requires all accessors utilize a PIV card while also logged onto the VA network through secure sites essentially a 2-factor authentication process. All VA employees accessing the system have had a background check.

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 as an identifier	Not used
Social Security Number (SSN) / VA File Number	Used as an identifier	Not used
Integrated Control Number (ICN)	Used as an identifier	Not used
Patient Identifier (PID)	Used as an identifier	Not used
Date of Birth (DOB)	Used as an identifier	Not used
Claim Number	Used as an identifier	Not used
Personal/Business Mailing Address	Used as an identifier	Not used
Personal/Business Phone Number	Used as an identifier	Not used
Personal/Business Email Address	Used as an identifier	Not used
Financial Information/Documentation	Used to audit beneficiary accounts	Not used
Bank Account Numbers	Used to audit beneficiary accounts	Not used

The information in the SF-FAST module will be used to identify the beneficiary and fiduciary.

The information and documentation will be electronically submitted to Fiduciary Hubs which are necessary for the oversight of VA beneficiaries allowing VA employees to validate and disposition accountings in a timely and efficient manner.

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

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

The SF-FAST module does not perform analytics. The module allows VA appointed Fiduciaries (External Users) to access SF-FAST to enter Accounting information on behalf of the Beneficiary they represent, upload supporting documentation electronically for Beneficiaries, and the ability to submit corrections and any missing information efficiently. VA Fiduciary employees will review the Accounting information uploaded by the Fiduciaries.

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.

VA Fiduciary employees will review the Accounting information uploaded by the Fiduciaries.

2.3 How is the information in the system secured?

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

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

Salesforce contractors assigned to SF-FAST, VA Employees, and VA appointed Fiduciaries will have access. Access is determined by permission sets/rights that are approved by the application owner, Pension and Fiduciary Services.

New users submit a request for access through the Digital Transformation Center (DTC). Digital Transformation Center (DTC) is the VA appointed governing body over VA use of the Salesforce platform and determine what is allowed or not allowed to go onto the production platform. The DTC assigns the request to the individuals who have admin access to the module and the access is then granted or denied based on the information the user provided. The DTC is then notified of the approval/disapproval and DTC takes action on the request based on the admin's response. Requests, approvals, and denials of access are recorded within Salesforce.

The application utilizes Salesforce Shield protect adhering to FIPS 140-2 encrypted connection protests data at rest. Data shared with VBMS-FID uses a REST Apex class.

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

PII in Salesforce applications is encrypted and each user that has access to the salesforce platform has to agree to the Privacy Information Security Agreement Rules of Behavior once a year that dictates how employees use/safeguard PII/PHI. Additionally, audits can be performed to track misuse or any prohibited use of PII/PHI. Any disciplinary actions for misuse of the information would be covered in VBA's privacy policy and by governing regulations. The use of the information is critical to the success of the mission and fully supports the USB's current priorities.

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

PII in Salesforce applications is encrypted and each user that has access to the salesforce platform has to agree to the Privacy Information Security Agreement Rules of Behavior once a year that dictates how employees use/safeguard PII/PHI. Additionally, audits can be performed to track misuse or any prohibited use of PII/PHI. Any disciplinary actions for misuse of the information would be covered in VBA's privacy policy and by governing regulations. The use of

the information is critical to the success of the mission and fully supports the USB's current priorities.

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?

Salesforce contractors assigned to SF-FAST, VA Employees, and VA appointed Fiduciaries will have access. Access is determined by permission sets/rights that are approved by the application owner, Pension and Fiduciary Services.

New users submit a request for access through the Digital Transformation Center (DTC). Digital Transformation Center (DTC) is the VA appointed governing body over VA use of the Salesforce platform and determine what is allowed or not allowed to go onto the production platform. The DTC assigns the request to the individuals who have admin access to the module and the access is then granted or denied based on the information the user provided. The DTC is then notified of the approval/disapproval and DTC takes action on the request based on the admin's response. Requests, approvals, and denials of access are recorded within Salesforce.

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

Salesforce contractors assigned to SF-FAST, VA Employees, and VA appointed Fiduciaries will have access. Access is determined by permission sets/rights that are approved by the application owner, Pension and Fiduciary Services.

New users submit a request for access through the Digital Transformation Center (DTC). Digital Transformation Center (DTC) is the VA appointed governing body over VA use of the Salesforce platform and determine what is allowed or not allowed to go onto the production platform. The DTC assigns the request to the individuals who have admin access to the module and the access is then granted or denied based on the information the user provided. The DTC is then notified of the approval/disapproval and DTC takes action on the request based on the admin's response. Requests, approvals, and denials of access are recorded within Salesforce.

2.4c Does access require manager approval?

Manager approval is required. Hub supervisors and Pension & Fiduciary (P&F) Service managers approve requests submitted for FAST access.

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

PII in Salesforce applications is encrypted and each user that has access to the salesforce platform has to agree to the Privacy Information Security Agreement Rules of Behavior once a year that dictates how employees use/safeguard PII/PHI.

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

PII in Salesforce applications is encrypted and each user that has access to the salesforce platform has to agree to the Privacy Information Security Agreement Rules of Behavior once a year that dictates how employees use/safeguard PII/PHI. Salesforce contractors assigned to SF-FAST, VA Employees, and VA appointed Fiduciaries will have access. Access is determined by permission sets/rights that are approved by the application owner, Pension and Fiduciary Services.

New users submit a request for access through the Digital Transformation Center (DTC). Digital Transformation Center (DTC) is the VA appointed governing body over VA use of the Salesforce platform and determine what is allowed or not allowed to go onto the production platform. The DTC assigns the request to the individuals who have admin access to the module and the access is then granted or denied based on the information the user provided. The DTC is then notified of the approval/disapproval and DTC takes action on the request based on the admin's response. Requests, approvals, and denials of access are recorded within Salesforce.

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
Personal/Business Address
Personal/Business Phone Number
Personal/Business Email
Financial Information/Documentation
Bank Account Numbers
SSN/VA File Number
Date of Birth (DOB)
Integrated Control Number (ICN)
Patient Identifier (PID)
Claim Number

3.2 How long is information retained?

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

Per SORN 58VA21/22/28 86 FR 61858, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, retention and disposal, paper documents received are scanned into VA's electronic document repository and subsequently destroyed after determining that the official record copy or original is in file.

Electronic records are not purged.

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

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

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

Yes

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

SF-FAST complies with all VA retention and disposal procedures. In accordance with SORN #: 58VA21/22/28 86 FR 61858, *Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA,* records are disposed in accordance with Records Control Schedule VB–1, Part 1 Section XIII, Item 13–052.100 (https://www.archives.gov/records-mgmt/grs) as authorized by NARA.

Item 13-052.100 - Destroy after determining that the official record copy or original is in file.

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.

Per SORN 58VA21/22/28 86 FR 61858, *Compensation, Pension, Education, and Vocational* Rehabilitation and Employment Records-VA. The Privacy Act of 1974 (5 U.S.C. 552a(e)(4)), is the legal authority to collect the information listed in question 1.1. The authority for maintenance of the system is Section 501(a), (b), and chapter 55 of Title 38, United States Code.

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.

The lower development environments for Salesforce do not allow the use of PII. For the SF-FAST module, test data is utilized/created. Because the configuration of the component does not have any validation against other VA systems of record, real Veteran data is not required to test the functionality of the system. Training for users is done in the lower environments and test data is used.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

Follow the format below:

Privacy Risk: The risk to maintaining data within the SF-FAST module is that longer retention times increase the risk that information can be compromised or breached.

Mitigation: To mitigate the risk posed by information retention, the SF-FAST Module adheres to the VA RCS 10-1. All electronic storage media used to store, process, or access records will be disposed of in adherence with the VA Directive 6500.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Benefit Gateway Service (BGS)	Identify the Veteran and Fiduciary for provision of Fiduciary Accounting Information	Name, address, phone number, email address, SSN or VA File #	Electronic – BGS Application Programming Interface (API)
Master Patient Index (MPI)	Identify the Veteran	Integrated Control Number (ICN), Veteran Name, SSN,	Electronic – MPIe API

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		VA File #, Address, DOB, Patient Identifier (PID)	
Veterans Benefits Management System – Fiduciary (VBMS-FID)	Updating the Veteran eFolder and the accounting audit tool.	Veteran Name, Address, Email Address, Phone, SSN, VA File #, Claim Number, DOB, Financial Information/Documentation, Bank Account Numbers, PID	Salesforce REST Apex class integration which will allow VBMS to pull data through DTC Integration Platform (DIP) middleware.; Files containing PII are converted to .pdf using DIP as a middleware prior to the files being transferred via the Claim Evidence API.

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: The risk is similar with any other systems that if the wrong person were to have access to the information, it could be used to obtain financial resources and negatively impact a beneficiaries' lives.

Mitigation: The Salesforce Government Cloud requires all accessors utilize a PIV card while also logged onto the VA network through secure sites essentially a 2-factor authentication process. All VA employees accessing the system have had full background checks. Information is only shared with approved internal systems. Security controls are in place to prevent

unauthorized access such as: access controls, authentication, and use of PIV. Audit logs in Salesforce are available to track any inappropriate internal sharing and/or disclosure.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can***	***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: There is no external sharing.

Mitigation: There is no external sharing.

Section 6. Notice

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

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

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

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

The following SORN covers FAST: SORN #: 58VA21/22/28 86 FR 61858, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA. The Privacy Act of 1974 (5 U.S.C. 552a(e)(4)), is the legal authority to collect the information listed in question 1.1. The authority for maintenance of the system is Section 501(a), (b), and chapter 55 of Title 38, United States Code.

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

The Privacy notice is provided prior to submission of the form. There is a link to the privacy policy and a checkbox next to it that must be selected before submitting the form. This link provides specific information on the Privacy Policy.

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

The Privacy notice is provided prior to submission of the form. There is a link to the privacy policy and a checkbox next to it that must be selected before submitting the form. This link provides specific information on the Privacy Policy.

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.

The use of SF-FAST is voluntary and there are no penalties or denial of services associated with declining to use the module. Users may submit information in the traditional formats: fax or mail. Individuals know that VA timeliness of processing the Financial Accounting Information will be affected when using mail or fax.

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.

The Privacy Policy must be viewed and accepted prior to submission of the form. Consent must be given to cover all bases.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Privacy Risk: A potential risk is if a user entered their own PII in part one question eight they may not realize that they are doing so.

Mitigation: SORN 58VA21/22/28 86 FR 61858, along with this PIA, acts as a means of notification to individuals that SF-FAST is retaining PII Data.

Section 7. Access, Redress, and Correction

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

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

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

End users (VA Appointed Fiduciaries of Veterans/Beneficiaries) submitting accountings in SF-FAST are only able to view what they have personally submitted.

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 data collected within SF-FAST is not exempt from FOIA/Privacy Act requests and would be handled by the centralized group processing VBA FOIA/Privacy Act requests.

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 data collected within SF-FAST is not exempt from FOIA/Privacy Act requests and would be handled by the centralized group processing VBA FOIA/Privacy Act requests.

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.

Corrections would go through the centralized group processing VBA FOIA/Privacy Act requests and that group would submit the request to P&F Service. If the Fiduciary who submitted the information is working with their VA employee and became aware of the incorrect information, they could provide this information to the VA employee via email or telephone call. If the information was submitted via a telephone call, the VA Employee would document the information utilizing the current VA policy for obtaining information.

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.

Corrections would go through the centralized group processing VBA FOIA/Privacy Act requests and that group would submit the request to P&F Service. A formal process has not yet been established. If the individual who submitted the information is working with the VA Fiduciary employee and became aware of the incorrect information, they could provide this information to the VA Fiduciary employee via email or telephone call. If the information was submitted via a telephone call, the VA Fiduciary employee would document the information utilizing the current VA policy for obtaining information.

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.

Veterans and authorized parties have a statutory right to request a copy of or an amendment to a record in VA's possession at any time under the Freedom of Information Act (FOIA) and the Privacy Act (PA). VA has a decentralized system for fulfilling FOIA and PA requests. The type of information or records an individual is seeking will determine the location to which a request should be submitted. For records contained within a VA claims folder (Compensation and Pension claims), or military service medical records in VA's possession, the request will be fulfilled by the VA Records Management Center. Authorized requestors should mail their Privacy Act or FOIA requests to: Department of Veterans Affairs, Claims Intake Center, P.O. Box 4444, Janesville,

WI 53547–4444, DID: 608–373–6690. For other benefits records maintained by VA (to include Vocational Rehabilitation & Employment, Insurance, Loan Guaranty or Education Service) submit requests to the FOIA/ Privacy Act Officer at the VA Regional Office serving the individual's jurisdiction. Address locations for the nearest VA Regional Office are listed at VA Locations Link. Any individuals who have questions about access to records may also call 1–800–327–1000. Information about how to contact Fiduciary services can be found here: https://www.benefits.va.gov/FIDUCIARY/contact-us.asp.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that individuals that enter information will not be able to access the information once submitted.

Mitigation: The external user, while they cannot directly access the information they enter, they can contact the VA using a FOIA request to obtain this information.

Section 8. Technical Access and Security

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

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

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

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

There are two groups of users for the SF-FAST module. VA appointed Fiduciaries are external users that gain access to the SF-FAST module by completing a self-registration form. External users are only able to submit accounting information on behalf of the Veteran/beneficiary they represent and cannot see anything else other than what they submit. The other group of users are VA employees from Fiduciary Service. These users can see incoming accounting submissions from the external Fiduciary users. Beneficiaries do not have direct access into the SF-FAST module within the Salesforce platform. The external user with access is the Fiduciary in charge of the financials of the beneficiary.

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?

There are two groups of users for the SF-FAST module. VA appointed Fiduciaries are external users that gain access to the SF-FAST module by completing a self-registration form. External users are only able to submit accounting information on behalf of the Veteran/beneficiary they represent and cannot see anything else other than what they submit. The other group of users are VA employees from Fiduciary Service. These users can see incoming accounting submissions from the external Fiduciary users. Beneficiaries do not have direct access into the SF-FAST module within the Salesforce platform. The external user with access is the Fiduciary in charge of the financials of the beneficiary.

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.

FAST can be accessed by external fiduciary users who have the ability to create and submit accountings. The external fiduciary users are only able to submit accounting information and can only see what they submit. VA employee users can see accounting submissions from the external fiduciaries.

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

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

Only VA contractors from the DTC will have access to the production environment. VA Contractors are required to complete the Privacy and Information Security Agreement yearly, also known as the Rules of Behavior. Signing the Rules of Behavior ensures proper conduct and management of sensitive information.

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.

No additional system specific privacy training is provided for end users of the SF-FAST module. All users are required to have the standard HIPAA and VA Privacy Information Security Awareness Rules of Behavior training.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 05-Apr-2023
3. *The Authorization Status:* Approved
4. *The Authorization Date:* 07-Aug-2023
5. *The Authorization Termination Date:* 06-Aug-2025
6. *The Risk Review Completion Date:* N/A
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 No or In Process, provide your ***Initial Operating Capability (IOC) date.***

Authorization and Accreditation has been completed for this system.

Section 9 – Technology Usage

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

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

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

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

Yes, SF-FAST utilizes Salesforce Government Cloud Plus. Salesforce Government Cloud Plus is hosted in the AWS GovCloud. The Salesforce Government Cloud Plus (SFGCP-E) is built on the underlying Salesforce Force.com that is hosted in a FedRAMP Certified FISMA High environment which is in the Amazon Web Services (AWS) GovCloud West. This software utilizes the PaaS Service of Salesforce Gov Cloud Plus. Application

Programming Interfaces (APIs), Salesforce REST Apex class integration, and DTC Integration Platform (DIP) middleware integrations allows dataflow between different systems.

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

Yes, VA has full ownership of the PII that will be used by the SF-FAST module. Contract agreement "Salesforce Subscription Licenses, Maintenance and Support", Contract Number: NNG15SD27B, Order Number: 36C10B23F0172

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.

Ancillary data is not collected by Salesforce. VA has full ownership over the data stored in SF-FAST.

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.

VA has full authority over data stored in SF-FAST.

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).

No robotic process automation (RPA) is used in this system.

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

ID	Privacy Controls
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.

DONTRELL WIGGINS

Digitally signed by DONTRELL WIGGINS
Date: 2024.11.05 14:11:04 -07'00'

Privacy Officer, Dontrell Wiggins

JAMES BORING

Digitally signed by JAMES BORING
Date: 2024.11.06 10:14:03 -05'00'

Information System Security Officer, James Boring

MICHAEL DOMANSKI

Digitally signed by MICHAEL DOMANSKI
Date: 2024.11.06 10:07:55 -05'00'

Information System Owner, Michael Domanski

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).

- Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA 58VA21/22/28 / 86 FR 61858 (https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf)
- Privacy, Policies, And Legal Information | Veterans Affairs

HELPFUL LINKS:

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

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

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

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

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