Privacy Impact Assessment for the VA IT System called:

Financial Support Application Enclave (FSAE)

Veterans Affairs Central Office (VACO)
VA Financial Services Center (FSC)

eMASS ID # 2495

Date PIA submitted for review:

4/18/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Pamela M. Smith	Pamela.Smith6@va.gov	512-937-4724
Information System Security Officer (ISSO)	Ronald Murray	Ronald.Murray2@va.gov	512-460-5081
Information System Owner	Jonathan Lindow	Jonathan.Lindow@va.gov	(512) 981-4871

Abstract

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

The Financial Services Center (FSC) Financial Support Application Enclave (FSAE) is a cloud-based communications network that support FSC users in their day-to-day operations. FSAE will host additional minor applications that may use PII of veterans, VA contractors and VA employees. The FSAE Enclave is located within the VA Enterprise Cloud Service enclave, the cloud service provider is Microsoft Azure Government (MAG).

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?

The Financial Services Center (FSC) Financial Support Application Enclave (FSAEs) is a communications network that supports FSC users in their day-to-day operations.

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

This system is continuously used during business and non-business hours, supporting many business processes within the VA FSC computing environment. The confidentiality, integrity, and availability of the FSC FSAE is critical, (i.e., ensuring that data is only received by the persons and applications that it is intended for, that data is not subject to unauthorized or accidental alterations, and that the resources are available when needed). Due to the sensitivity of this information system, all personnel with System Administration rights and roles require an elevated background investigation to fulfill their duties. The information processed by the FSC FSAE is sensitive but unclassified (SBU). It is considered sensitive information as defined by the
Privacy Act of 1974, the Health Insurance Protection and Accountability Act (HIPAA), and the Federal Information Processing Standard (FIPS) 199. The estimated number of stations total entries whose information is stored on the FSC's FSAE system is 3,357,793.

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

The Financial Services Center

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?

Application name	Expected number of individuals whose information is stored in the system	A brief description of the typical client or affected individual	A general description of the information in the IT system	Purpose for collecting this information
Automated Vendorizing Input System (AVIS)	There is no information on individuals in this system. Only organizational information.	A typical client is VA stations.	FMS AVIS provides a tool to VHA agents to update the Veterans information to FMS with minimal support from the Vendorizing team. Vendorizing team will be involved in the process to resolve exception, if any.Creates/modifies the information for vendorized Veterans who get FMS payments. The application creates FMS transactions for these Vendor file updates. It also receives back an update for the purpose of processing rejections.The FMS AVIS service sends veteran updates or additions to FMS for the vendor files.	VA stations can add veteran banking information to FMS.

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

See Above Chart

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

See Above Chart

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?

Microsoft Azure Government (MAG)

3. Legal Authority and SORN

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

Legal authority to operate: Budget and Accounting Act of 1950; General Accounting Office Title 8, Chapter #3; Social Security Account Number (SSAN) is used to index, and store pay affecting documents. Also, the use of the SSN is required from the customer for IRS tax reporting and cannot be eliminated. It is also required for security clearance processing. Authorized under Executive Orders 9397, 10450, 10865, 12333, and 12356; sections 3301 and 9101 of title 5, U.S. Code; Homeland Security Presidential Directive 12.

SORN:13VA047 Individuals Submitting Invoices-Vouchers For Payment-VA
https://www.govinfo.gov/content/pkg/FR-2020-04-23/pdf/2020-08611.pdf
131VA047 Purchase Credit Card Program-VA
https://www.govinfo.gov/content/pkg/FR2021-09-21/pdf/2021-20362.pdf

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

No

4. System Changes

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

No

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

No

Section 1. Characterization of the Information

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

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

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

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

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

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

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

Add Additional Information Collected but Not Listed Above Here:

- Banking Information
- Account Information
- Zip Code

PII Mapping of Components (Servers/Database)

Financial Support Application Enclave consists of 1 key component (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 < Financial Support Application Enclave > 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.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
FSC Vendor Services	Yes	Yes	•Veteran Name, •Veteran Address • Bank Account Number • Veteran Vendor Number (Social Security Number) • Bank Name • Bank Routing Number	Used to create and modify the information for vendorized Veterans who get Financial Management System (FMS) payments. Additionally, it is used to process rejections.	Access control including role-based access, authentication Safeguards, and configuration management, etc.

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?

AVIS: Business rules to process vendor file form (10091) requests have been defined by working with process subject matter experts, implemented in the system, and verified against existing data FSC Vendor Services that is periodically sync'd with the relevant system of record. (The FSC Data Depot)

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.

FSC systems load data from designated systems of record. This is approach reduce the number of locations where PHI and PII is stored which mitigates the risk of the information being compromised.

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

Systems do not create information only display it.

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?

FSAE does not collect any information directly from individuals. The information collected comes directly from FSC Vendor Services via script or Application Programming Interface (API)

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?

OMB Approved No. 2900-0846

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.

System and Online Form Submission is verified through background investigations, as the information is needed only for VA Employees and/or VA Contractors. For information collected from other VA and VA FSC systems, verification of data accuracy is done within the applications sharing the data with the FSAE. There is no contract requiring data to be checked for accuracy on the FSAE System. For information collected from other IT systems, the information is transmitted using a FIPS validated encryption module, which verifies by using hash algorithms that the data has not been corrupted.

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?

FSAE does not check for accuracy of data received through FSCDataDepot

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

Budget and Accounting Act of 1950; 38 USC 5101 (C); Social Security Account Number (SSAN), also known as Social Security Number (SSN), is used to index and store pay-affecting documents. Also, the use of the SSAN is required from the customer for IRS tax reporting and cannot be eliminated. It is also required for security clearance processing. Authorized under Executive Orders 9397, 10450, 10865, 12333, and 12356; sections 3301 and 9101 of title 5, U.S. Code; Homeland Security Presidential Directive 12.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: Sensitive Personal Information may be released to unauthorized individuals.

Mitigation: FSAE system adheres to information security requirements instituted by the VA Office of Information Technology (OIT). FSAE system relies on information previously collected by the VA from individuals. Both contractor and VA employees are required to take Privacy, HIPAA, and information security training annually. FSAE and file access is granted only to those with a valid need to know. The Microsoft Windows systems are updated and patched to the highest extent possible for the maximum available security assurance using Azure Update Management service. System logs are sent to Azure Log Analytics for monitoring and analysis. This also includes continuous Passive Vulnerability Scanning (PVS) information. CA Unified Infrastructure Management (CA UIM) software monitors and manages networks and systems Microsoft Azure Web Application Firewall (WAF) is used to protect web applications by filtering traffic to prevent botnet clients, Distributed Denial of Service (DDoS), and web user account takeover threats. EO's

Technical Security Service Line also provides centralized network security edge monitoring and protection using Intrusion Prevention System (IPS) and Malware Protection System (MPS) across all EO data centers in addition to the VA-Network and Security Operations Center (NSOC) provided security perimeter procedures.

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	for vendor, beneficiary, and entitlement payments, and for processing background security clearances and Admin/HR actions	Not used
Social Security Number	for processing background security clearances	Not used
Mailing Address	for vendor, beneficiary, and entitlement payments, and for processing background security clearances	Not used
Zip Code	for vendor, beneficiary, and entitlement payments, and for processing background security clearances	Not used
Financial Account Information	for vendor, beneficiary, and entitlement payments	Not used
Banking Information	Used to verify and validate customer information when managing customer calls from vendors.	Not used
Account Information	Used to verify and validate customer information when managing customer calls from vendors.	Not used

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

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 FSC FSAE is the backbone of communications for transmitting and receiving data. It supports the following minor applications:

FMS Automated Veteran Input System (FMS AVIS): provides a tool to Veterans Health Administration (VHA) agents to update the Veterans information to FMS with minimal support from the Vendorizing team. Vendorizing team will be involved in the process to resolve exceptions, if any.

FMS AVIS Creates/modifies the information for vendorized Veterans who get FMS payments. The application creates FMS workflow transactions for these Vendor file updates. It also receives back an update for the purpose of processing rejections. The FMS AVIS service sends updates for vendorized veterans that are already have existing vendor files in the FMS system.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

The new information created from the minor FSAE applications support the accuracy of the vendor file processes and supports downstream financial claims-based actions. It also supports Veteran's healthcare activities, VA employee financial activities, and payments to vendors that provide services to the VA. The information will be available once it's been reviewed and approved by the system or Vendorizing team. All information will be stored in current user record.

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?

Data in FSAE is encrypted at rest and in transit.

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

Role Based Access Controls limit access to Social Security Numbers (SSN) to only those roles that need access to SSN. SSN is masked for employee vendor, shows last 4 only, on confirmation screen, while SSN which comes in attachment for new employee bank set up is not masked.

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

Role Based Access Controls limit access to SSN to only those roles that need access to SSN. SSN is masked for employee vendor, shows last 4 only, on confirmation screen, while SSN which comes in attachment for new employee bank set up is not masked.

The Separated Employee Retirement (SER) users are Access to PII is limited by role

assignment, which is completed based on user role. Roles are assigned via SSOi and IAM provisioning process, where roles can be provided and loaded into the system for 104 stations.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

Access is determined based on he/she role and individual must complete appropriate training.

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

Yes

2.4c Does access require manager approval?

Yes

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

Yes

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

FSC ISSO, Privacy Officer, Product owner for each application.

Section 3. Retention of Information

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

3.1 What information is retained?

*Identify and list all information collected from question 1.1 that is **retained** by the system.*

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

The following data elements reside on the FTG for purposes of, but not limited to, making payments to vendors, beneficiaries, and medical providers; making entitlement payments to VA employees and Veterans; processing new employee background investigations; and processing Administrative and Human Resources-related actions on organizational employees.

Name—for vendor, beneficiary, and entitlement payments; for processing background security clearances; and Admin/HR actions
Social Security Number—for processing background security clearances
Mailing Address—for vendor, beneficiary, and entitlement payments, and for processing background security clearances
Financial Account Information—for vendor, beneficiary, and entitlement payments
Banking Information.
Account Information.

3.2 How long is information retained?

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

Records are retained as required per National Archivist and Records Administration (NARA) standards (Reference: GRS Schedule 1.1, Item #10). Destroy 6 years after final payment or cancellation, but longer retention is authorized if required for business use. User access form (9957) data is retained for 7 years as required by General Record Schedule (GRS) 6.1: Accountable Officers' Accounts Records for each claim as they are recorded separately. https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

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?

Each service has developed file plans identifying what records they are maintaining. Approved NARA GRS are identified, and specific retention guidelines are documented and followed in accordance with VA Handbook 6300.1, Records Management Procedures. NARA GRS 1.1 item #10 (Disposition Authority DAA-GRS-2013-0003-0001) identifies those records be maintained for the specified retention period.

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

All guidance is located at https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf under Records Management Regulations, Policy, and Guidance.

3.4 What are the procedures for the elimination or transfer of SPI?

Explain how records are destroyed, eliminated or transferred to NARA at the end of their mandatory retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.? This question is related to privacy control DM-2, Data Retention and Disposal.

Electronic records are retained as long as required (GRS Schedule 1.1, Item #10), and are destroyed in accordance with NARA disposition instructions. [Destroy 6 years after final payment or cancellation, but longer retention is authorized if required for business use.]

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

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.

Yes, the VA Financial Services Center uses techniques to minimize the risk to privacy by disallowing the use of PII for research/testing/training. Our Information System Security

Officers (ISSOs) enforce the policy that the only environments that can have live data is pre-prod and prod. No exceptions. Per VA Handbook 6500, security control SA-11: Developer Security Testing states: (c) Systems under development should not process "live data" or do any real processing in which true business decisions will be based. Test data that is de-identified should be used to test systems and develop systems that have not yet undergone security A&A. Furthermore, systems that are in development (pilot, proof-of-concept, or prototype) should not be attached to VA networks without first being assessed and authorized.

Additionally, the FSC Information Technology Service is developing a Standard Operating Procedure (SOP) that describes key procedures and processing steps that Financial Services Center (FSC) Information Technology Service (ITS) functional and/or project teams must follow when requesting production datasets for using in test or non-production environments. This process document outlines key tasks and responsibilities as relates to the proposal process of using production data for testing purposes. It establishes the procedures required to request permission to use live or production data, whether in original or altered form, to test an Information Technology (IT) system or project at the FSC.

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: There is a risk that the information maintained by the FSC FSAE will be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation: In addition to collecting and retaining only information necessary for fulfilling the VA mission, the disposition of data housed in FSC FSAE is based on standards developed by the National Archives Records Administration (NARA). This ensures that data is held for only as long as necessary.
The Records Manager ensures data retention policies and procedures are followed. The Privacy Officer, Information System Security Officer, and Chief Information Officer monitor controls to mitigate any breaches of security and privacy.

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***
OIT – FMS – under FMS AVIS	Allows a user to register to the system and see reports regarding the users	• Veteran Name, • Veteran Address • Veteran Social Security Number	Secure FTP via VLTrader

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*
	work list, reports of work list by station number. Admin User can add/edit/delete users from this site and change the workstations of the user	• Bank Account Number • Bank Name • Bank Routing Number	

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: Privacy information may be released to unauthorized individuals.

Mitigation: FSAE system adheres to information security requirements instituted by the VA Office of Information Technology (OIT). Both contractor and VA staff are required to take Privacy, HIPAA, and information security training annually. Information is shared in accordance with VA Handbook 6500 updated February 24th, 2021, Information Security Program. File/folder access granted only to those with a valid need to know.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
NA	NA	NA	NA	NA

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 a risk of exposure of sensitive information when transferring from VA systems to Treasury which is an outside source. Unauthorized exposure of sensitive data may result in privacy and security breaches.

Mitigation: Treasury shared a certificate which is installed on our servers to perform a handshake and the data will be transmitted over https which is secured.

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 FSC system does not collect information directly from individuals.

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

The SORN is provided to the public.

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 provided SORN explains the reason, purpose, authority, and routine uses of the collected information is adequate to inform those affected by the system that their information has been collected and is being used appropriately.

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 FSC FSAE does not collect information directly from individuals.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses, or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

The FSC FSAE does not collect information directly from individuals.

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: There is a risk that Veterans and other members of the public may not know that Financial Support Application Enclave (FSAE) systems exist or that it collects, maintains, and/or disseminates PII and another SPI about them.

Mitigation: FSC mitigates this risk by ensuring we provide an individual's notice of information collection and notice of the system's existence through the methods discussed in question 6.1.

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.***

The FSC FSAE system does not collect PII/PHI information directly from individuals. Nevertheless, individuals may always access their information via Freedom of Information Act (FOIA) and Privacy Act procedures. VA employees may access their information by contacting their servicing HR office.

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)?

FSAE is not exempt from the access provisions of 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?

FSAE is a Privacy Act system.

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.

Veterans can correct/update their information online via the VA's eBenefits website: https://www.ebenefits.va.gov
VA employees may access their information by contacting their servicing human resources office.

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 wishing to correct their medical information would follow Veterans Health Administration (VHA) processes/procedures as VHA maintains the system of record. Individuals may always access their information via Freedom of Information Act (FOIA) and
Privacy Act procedures. Please use the following link to access FOIA: Freedom Of Information Act FOIA (va.gov). VA employees may access their information by contacting their servicing HR office.

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 can correct/update their information online via the VA's eBenefits website:
https://www.ebenefits.va.gov

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 whose records contain incorrect information may not receive timely correspondence or services from the facility, e.g., incorrect information in a request for travel reimbursement could result in inability to generate proper payment.

Mitigation: FSC FSAE mitigates the risk of incorrect information in an individual's records by authenticating information when possible, using the resources discussed in Question 1.5.
Additionally, FSC FSAE's staff identifies incorrect information in individual records during payment transaction processing. Staff are also informed of the importance of maintaining compliance with VA Release of Information (ROI) policies and procedures and about the importance of remaining alert to information correction requests.

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?

Individuals receive access to the FSC FSAE systems by gainful employment in the VA or upon being awarded a contract that requires access to GSS and VISTA systems. Upon employment, the Office of Information & Technology (OIT) creates computer and network access accounts as determined by employment positions assigned. Users are not assigned to software packages or network connections that are not part of their assigned duties or within their assigned work area. Supervisors are required to review and approve an individual's initial and additional requests for access. Approval process is documented and maintained by the Information Technology (IT) office and the Information System Security Officer (ISSO).

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?

All applications under FSAE are internal.

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.

Separation of duties matrix is used to identify user's role and determine their level of access:

- User: read only
- System admin: read and write
- Database admin: read and write
- Application Admin: read and write
- VA Cloud Broker: read and write
- Managers: read and write
- Approvers: read and write

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.

Contractors will have access to FSC FTG system. Contracts are reviewed annually by the Contracting Officer Representative (COR). Clearance levels are determined by the COR and position sensitivity level and risk designation. Access is reviewed annually, and verification of Cyber Security and Privacy training is validated by the COR.

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.

Privacy and Information Security Awareness and Rules of Behavior (Talent Management System course #10176) is required for all Federal and Contractor personnel that require access to the VA Network. Annual training compliance is closely monitored.

Other required Talent Management System courses monitored for compliance:

- VA 10203: Privacy and HIPAA Training
- VA 3812493: Annual Government Ethics

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

8.4a If Yes, provide:

1. *The Security Plan Status: New system*
2. *The System Security Plan Status Date: New system*
3. *The Authorization Status: New system*
4. *The Authorization Date: New system*
5. *The Authorization Termination Date: New system*
6. *The Risk Review Completion Date: New system*
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.***

N/A as there is no Initial Operating Capability (IOC) date.

Section 9 – Technology Usage

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

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

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

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

FSAE is in the Veterans Administration Enterprise Cloud (VAEC). The name of provider is Microsoft Azure Government (MAG) Information as a Service (IaaS)

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.*

New system and N/A

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

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also

involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.
This question is related to privacy control DI-1, Data Quality.

New system and N/A

9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?
What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

New system and N/A

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

New system and N/A

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

PAMELA SMITH

Digitally signed by PAMELA SMITH
Date: 2024.05.23 13:23:38 -05'00'

Privacy Officer, Pamela M. Smith

RONALD MURRAY

Digitally signed by RONALD MURRAY
Date: 2024.05.23 14:05:35 -05'00'

Information System Security Officer, Ronald Murray

JONATHAN LINDOW

Digitally signed by JONATHAN LINDOW
Date: 2024.05.23 14:26:15 -05'00'

Information System Owner, Jonathan Lindow

APPENDIX A-6.1

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

HELPFUL LINKS:

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

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

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

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

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