Privacy Impact Assessment for the VA IT System called:

Financial Management Business Transformation (FMBT) Data Estate

VACO

Financial Services Center (FSC) / Financial Management Business Transformation (FMBT)

eMASS ID # 209

Date PIA submitted for review:

2/9/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Pamela M. Smith	Pamela.Smith6@va.gov	(512)-386-2246
Information System Security Officer (ISSO)	Ronald Murray	Ronald.Murray2@va.gov	(512)-460-4081
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?".

Financial Management Business Transformation (FMBT) Data Estate is a multi-environment system made up of third-party tools intended for business intelligence financial reporting and to store archivable data/records from interfacing financial systems until final disposition. The main interfacing system is the Integrated Financial Management and Acquisition System (iFAMS). Like iFAMS, Data Estate is a cloud-based system hosted within the Veterans Affairs (VA) Enterprise Cloud Service enclave and cloud service provider is Microsoft Azure Government (MAG). MAG has been certified as a FedRAMP High cloud and due to the expected volume of data, Data Estate has been categorized as FISMA High. Data Estate data is covered under the notice 13VA047, Individuals Submitting Invoices-Vouchers for Payment and Accounting Transactional Data. Its system of records comprises of financial, accounting, benefit and, transactional data across the VA enterprise nationwide. Use case constitutes VA meeting financial management objectives for veterans, veteran health providers, and dependents. Data from thousands of veterans and their dependents, VA employees, VA contractors, and members of the public are collected and stored in this system. VA retains ownership of the data use, storage, security, access, sharing, and controls all of engagement concerning data. Data Estate will host and share data from the following internal data sources: iFAMS, Financial Management System (FMS), Financial Reporting Data Warehouse (FRDW), Financial Reporting System (FRS), Human Resources – Payroll Application Services (HR-PAS), Credit Card System (CCS), and Invoice Payment Processing System (IPPS).

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?

1.A.1 FMBT Data Estate is owned by Financial Service Center

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

1.B.1 Data Estate intends to provide a business intelligence reporting and archiving environment that enables VA to meet financial management objectives and comply with VA financial management policies and federal regulations. As this is a national system, Data Estate will supply storage and financial reporting capabilities across all administrations, facilities, and offices throughout VA. This system will facilitate VA compliance with federal financial reporting obligations and to adhere to legal disposition of records in accordance to MP-4, Part X Change 2, dated May 26, 1982 and 10-1 VHA RCS. Veterans and vendors/customers that do business with Veterans Affairs sensitive information is

required to execute legal required receivables and payments through the United States Treasury and financial system entities. Legal authorities for which this system collects SSN's Federal Managers Financial Act (FMFIA); OMB Circular A-130, A-127, and A-123; and Executive Order 9397.

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

1.C.1 Data Estate is VA Owned and VA Operated. Data Estate is categorized as FISMA high, and Microsoft Azure is certified as a FedRAMP high cloud. The legal authority to operate this system is Public Law 100-527, 100th Congress. SORN VA13047 is being revised and is in concurrence for approval and subsequent publication in the Federal Register. Data Estate will not be operated in more than one site; this system is in the VA enterprise cloud (VAEC) within cloud service provider, Microsoft Azure. Data Estate will inherit all FedRAMP certification documentation, processes, and will follow all data custodial rights negotiated by VA when Microsoft Azure Cloud service provider was contracted by the department.

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?

1.D.1 The expected number of individuals is directly correlated to the number of vendorized individuals in IFAMS. Any individual that receives payments, grants, housing loans, etc. from VA will be built as a vendor in IFAMS and then that information is replicated over to Data Estate. Therefore, the number of individuals is conceptually in the hundreds of thousands to millions. Examples of the types of individuals who could be vendorized to receive payments: Veterans and their family members, individuals operating as a business and invoicing VA, individuals who are operating on behalf of VA and receiving payment, researchers.

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

1.E.1 Data Estate general description of PII being collected and maintained are as follows:

•Names of recipients
•Email address
•Mailing address
•Banking account number electronic funds transfer/Automated Clearing House (EFT/ACH) routing information from individual
•Financial account information
•Credit Card Numbers,
•Taxpayer Identification Number (TIN)
•Social security numbers/Tax ID of government employees,
•Credit card numbers
•Internet IP Addresses
•Retirement Information
•Life Insurance Information
•Medicare Information

•Health Insurance Information
•Voluntary Separation Information
•Incentive Award
•Senior Executive Service Award
•Travel Savings Award
•Relocation Incentive
•Recruitment Incentive
•Hazard Pay
•Student Loan Repayment
•Supervisory Differential
•Vendor ID
•Sole proprietorship first name
•Last name
•Middle name
•Tax ID number
•Financial Institute
•Account number ABA Routing ID
•Account
•Lockbox number
•EFT Waiver
•Remittance Name
•Remittance Address
•Remittance City
•Remittance State
•Remittance Zip
•Remittance Country
•Accounts Receivable First Name
•Accounts Receivable Last Name
•Accounts Receivable Middle Name
•Merchant ID

The reason for collection/storage of PII is due to the following: Public Law 100-527, 100th Congress-SSN's Federal Managers Financial Act (FMFIA);OMB Circular A-130, A-127,and A-123; and Executive Order 9397. Information is collected as an archiving and financial reporting system across all administrations, facilities, and offices throughout VA. This system will facilitate VA compliance with federal financial reporting obligations and to adhere to legal disposition of records.

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

1.F.1 Office of Financial Services (FSC); Data Elements: SSN, Stub Name, Retirement Indicator, Retirement, Social Security, Life Insurance, Medicare, Health Insurance, Voluntary Separation Incentive Award, Incentive Award, Senior Executive Service Award, Travel Savings Award, Relocation Incentive, Recruitment Incentive, Hazard Pay, student Loan Repayment, Supervisory

Differential; Method of Transmission: Secure File Transfer Protocol Server (SFTP)

1.F.2 Office of Finance/ Financial Management Services (FMS); Data Elements: Name, SSN(s), email address, mailing address, financial account information, banking account number from individual, banking account number from Vendor, Agency banking account number, Electronic Funds Transfer /Automated Clearing House routing information, Credit Card Numbers, Taxpayer Identification Number (TIN), and data required to process receivables and payments through the United States Treasury and financial system entities; Method of Transmission: SFTP Server

1.F.3 FSC/ Charge Card System (CCS); Data Elements: User ID Title User ID Vendor Address Code Vendor Code; Method of Transmission: CCS is an interfacing financial system.

1.F.4 FSC/ Financial Report System (FRS); Data Elements: Vendor Code Vendor Address Code Vendor Name User ID; Method of Transmission: FRS is an interfacing financial system.

1.F.5 FSC/ Invoice Payment Processing System (IPPS); Data Elements: Vendor Name; Method of Transmission: IPPS is an interfacing financial system.

1.F.6 FSC / Financial & Acquisition Management System (IFAMS): Names of recipients, Email address, Mailing address, Banking account number electronic funds transfer/Automated Clearing House(EFT/ACH)routing information from individual, Financial account information, Credit Card Numbers,, Taxpayer Identification Number (TIN), Social security numbers/Tax ID of government employees,, Credit card numbers, Internet IP Addresses, Retirement Information, Life Insurance Information, Medicare Information, Health Insurance Information, Voluntary Separation Information, Incentive Award, Senior Executive Service Award, Travel Savings Award, Relocation Incentive, Recruitment Incentive, Hazard Pay, Student Loan Repayment, Supervisory Differential, Vendor ID, Sole proprietorship first name, Last name, Middle name, Tax ID number, Financial Institute, Account number ABA Routing ID, Account, Lockbox number, EFT Waiver, Remittance Name, Remittance Address, Remittance City, Remittance State, Remittance Zip, Remittance Country, Accounts Receivable First Name, Accounts Receivable Last Name, Accounts Receivable Middle Name, Merchant ID

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?

1.G.1 Data Estate will not be operated in more than one site. This system is in the VA enterprise cloud (VAEC) within cloud service provider, Microsoft Azure. Data Estate will inherit all FedRAMP certification documentation, processes, and will follow all data custodial rights negotiated by VA when Microsoft Azure Cloud service provider was contracted by the department. Data Estate is categorized as FISMA high, and Microsoft Azure is certified as a FedRAMP high cloud. The legal authority to operate this system is Public Law 100-527, 100th Congress. SORN VA13047 is being revised and is in concurrence for approval and subsequent publication in the Federal Register.

3. Legal Authority and SORN

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

1.H.1 Department of Veterans Affairs Act, Public Law 100-527, 100th Congress

1.H.2 Federal Managers Financial Act (FMFIA)

1.H.3 OMB Circular A-130, A-127, and A-123

1.H.4 Executive Order 9397, Numbering System for Federal Accounts Relating to Individual Persons

1.H.5 VA financial policy and procedures

1.H.6 SORN Notice 13VA047, Individuals Submitting Invoices – Vouchers for Payment and Accounting Transactional Data

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?

1.I.1 The SORN requires no amendments or revisions. The SORN covers cloud usage via the VA managed enterprise service cloud enclave.

4. System Changes

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

1.J.1 No

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

1.K.1 No

Section 1. Characterization of the Information

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

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

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

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

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

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

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

Other PII/PHI data elements:

- Banking account number from individual
- Banking account number from Vendor
- Agency banking account number
- Electronic Funds Transfer /Automated Clearing House routing information
- Credit Card Numbers
- Data required to process receivables and payments through the United States Treasury and financial system entities.
- Insurance Information
- Medicare Information
- Health Insurance Information
- Voluntary Separation Information
- Incentive Award
- Senior Executive Service Award
- Travel Savings Award
- Relocation Incentive
- Recruitment Incentive
- Hazard Pay
- Student Loan Repayment
- Supervisory Differential
- Vendor ID
- Sole proprietorship first name, Last name, Middle name,
- Tax ID number
- Financial Institute

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

- Account number ABA Routing ID
- Lockbox number
- EFT Waiver Remittance Name, Remittance Address, Remittance City, Remittance State, Remittance Zip, Remittance Country
- Accounts Receivable First Name, Accounts Receivable Last Name, Accounts Receivable Middle Name
- Merchant ID

PII Mapping of Components (Servers/Database)

FMBT Data Estate consists of 2 key components (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Financial Management Business Transformation (FMBT) Data Estate and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
ifams_adhoc_prod	**Yes**	**Yes**	Names of recipients • Email address • Mailing address • Banking account number electronic funds transfer/Automated Clearing House (EFT/ACH) routing information from individual • Financial account information • Credit Card Numbers, • Taxpayer Identification Number (TIN) • Social security	This database contains a subset of tables from the Integrated Financial Acquisition Management System (iFAMS) database. PII is collected to facilitate VA compliance with federal financial reporting obligations and to adhere to legal disposition of records.	Access is individually controlled according to job functions. Network accessibility is severely limited to prevent unauthorized use. High impact security controls over system resources

			numbers/Tax ID of government employees, • Credit card numbers Internet IP Addresses • Retirement Information • Life Insurance Information • Medicare Information • Health Insurance Information • Voluntary Separation Information • Incentive Award • Senior Executive Service Award • Travel Savings Award • Relocation Incentive • Recruitment Incentive • Hazard Pay • Student Loan Repayment • Supervisory Differential • Vendor ID • Sole proprietorship first name • Last name • Middle name • Tax ID number • Financial Institute • Account number ABA Routing ID • Account • Lockbox number • EFT Waiver Remittance Name • Remittance Address • Remittance City • Remittance State • Remittance Zip • Remittance Country • Accounts Receivable First Name • Accounts	iFAMS is VA's implementation of the CGI Momentum Financials® product. Momentum is a commercial off-the-shelf (COTS) software solution. The product provides budgeting, acquisition and financial management capabilities specifically designed for the Federal Government -Public Law 100-527, 100th Congress -SSN's Federal Managers Financial Act (FMFIA); -OMB Circular A-130, A-127, and A-123; Executive Order 9397	and parent system. FedRamp High designation requires stringent security controls for system resources.

			Receivable Last Name • Accounts Receivable Middle Name • Merchant ID		
vac21sqlfmt200/ FMBT_Reporting	**Yes**	**Yes**	• Employee Name • Monthly payment information	This database contains a subset of data from the Financial Management System (FMS) and Payroll Application Services (HR-PAS) system. The data is used for combined FMS / IFAMS Reporting required by law and for continuity of business operations. -Public Law 100-527, 100th Congress -SSN's Federal Managers Financial Act (FMFIA); -OMB Circular A-130, A-127, and A-123; Executive Order 9397	Access is individually controlled according to job functions. Network accessibility is severely limited to prevent unauthorized use. High impact security controls over system resources and parent system. FedRamp High designation requires stringent security controls for system resources.

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

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

Information is provided by internal source data systems and not the individual. The data sources include: iFAMS, Financial Management System (FMS), Financial Reporting Data Version Date: January 2, 2019, Page 8 of 74 Warehouse (FRDW), Financial Reporting System

(FRS), Human Resources – Payroll Application Services (HR-PAS), Credit Card System (CCS), and Invoice Payment Processing System (IPPS).

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.

FMBT Data Estate aggregates data from other systems to provide live, operational reporting from enterprise BI tooling, as well as secure storage and reporting for business operations.

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

N/A as the system does not create information.

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?

Data is being collected by internal interfacing systems iFAMS, Financial Management System (FMS), Financial Reporting Data Warehouse (FRDW), Financial Reporting System (FRS), Human Resources – Payroll Application Services (HR-PAS), Credit Card System (CCS), and Invoice Payment Processing System (IPPS).

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

N/A, there is no physical form collection conducted or information sourced from physical forms that is ingested into Data Estate.

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.

VA will take reasonable steps through system configurations and administrative processes and procedures to confirm and affirming the accuracy of PII being collected. The types of measures taken to protect data quality will be based on the nature and context of the PII, how it is to be used, and how it was obtained. Measures taken to validate the accuracy of PII that is used to make determinations about the rights, benefits, or privileges of individuals under federal programs will be more comprehensive than those used to validate less sensitive PII. Additional steps will be necessary to validate PII that is obtained from sources other than individuals or the authorized representatives of individuals. Automated, routine system checks occur between source and target systems to ensure row counts and summarizations are consistent between them.

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?

FMBT Data Estate does not check for accuracy of individuals' data. Any corrections from data collected in upstream systems such as IFAMS or FMS would automatically be merged and corrected in Data Estate.

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

- Department of Veterans Affairs Act, Public Law 100-527, 100th Congress
- Federal Managers Financial Act (FMFIA)
- OMB Circular A-130, A-127, and A-123
- Executive Order 9397, Numbering System for Federal Accounts Relating to Individual Persons
- VA financial policy and procedures
- SORN Notice 13VA047, Individuals Submitting Invoices – Vouchers for Payment and Accounting Transactional Data

1.6 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>

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:

<u>Principle of Purpose Specification:</u> 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: Information being collected, used, stored, and disseminated is directly related to financial reporting capabilities across all administrations, facilities, and offices throughout VA.
Privacy risks are surrounding the sensitivity of the information being collected, maintained, and stored. There is a breach risk in the volume of data being stored. If data is exposed the department would be in grave risk for financial hardship and damaged reputation.

Mitigation: Data Estate is being hosted in Microsoft Azure certified as a high impact cloud. FedRAMP High impact controls surrounding the environment will add on an extra layer of protection through confidentiality, integrity, and availability for Data Estate information. Additionally, as an agency requirement all employees with access to this application would have to complete the VA Privacy and Information Security Awareness Training and Rules of Behavior and Departmental Privacy training.

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
Student Loan Repayment	Used for benefit / invoicing / payment distribution	Not used
Supervisory Differential	Used for benefit / invoicing / payment distribution	Not used
Sole Proprietor Remittance State	Used to locate individual	Not used
Sole Proprietor Zip	Used to locate individual	Not used
Sole Proprietor Country	Used to locate individual	Not used

Accounts Receivable First Name	Used to identify individual / Sole Proprietor	Not used
Accounts Receivable Last Name	Used to identify individual / Sole Proprietor	Not used
Accounts Receivable Middle Name	Used to identify individual / Sole Proprietor	Not used
Merchants ID	Used for benefit / invoicing / payment distribution	Not used
Banking account number from Vendor	EFT/ACH Used for benefit / invoicing / payment distribution	Not used
Agency banking account number	Used for benefit / invoicing / payment distribution	Not used
Electronic Funds Transfer /Automated Clearing House routing information	EFT/ACH Used for benefit / invoicing / payment distribution	Not used
Data required to process receivables and payments through the United States Treasury and financial system entities	EFT/ACH Used for benefit / invoicing / payment distribution	Not used
Insurance Information	Used for benefit /processing/ invoicing / payment distribution	Not used
Medicare Information	Used for benefit /processing/ invoicing / payment distribution	Not used
Health Insurance Information	Used for benefit /processing/ invoicing / payment distribution	Not used
Voluntary Separation Information	Used for benefit / invoicing / payment distribution	Not used
Incentive Award	Used for benefit / invoicing / payment distribution	Not used
Senior Executive Service Award	Used for benefit / invoicing / payment distribution	Not used
Travel Savings Award	Used for benefit / invoicing / payment distribution	Not used
Relocation Incentive	Used for benefit / invoicing / payment distribution	Not used
Recruitment Incentive	Used for benefit / invoicing / payment distribution	Not used

Hazard Pay	Used for benefit / invoicing / payment distribution	Not used
Name of recipient	Used to identify individual / Sole proprietor	Not used
Email address	Used to contact individual	Not used
Mailing Address	Used to locate individual	Not used
Bank Account Number	EFT/ACH Used for benefit / invoicing / payment distribution	Not used
Financial Account Information	Used for benefit / invoicing / payment distribution	Not used
Credit Card Numbers	Used for benefit / invoicing / payment distribution	Not used
TIN	Used for benefit / invoicing / payment distribution	Not used
SSN	Used to identify individual / Sole Proprietor	Not used
Internet IP Address	Used to identify individual / Sole Proprietor	Not used
Sole Proprietor First Name	Used to identify individual / Sole Proprietor	Not used
Sole Proprietor Last Name	Used to identify individual / Sole Proprietor	Not used
Sole Proprietor Middle Name	Used to identify individual / Sole Proprietor	Not used
Sole Proprietor TIN	Used for benefit / invoicing / payment distribution	Not used
Sole Proprietor Financial Institute	Used for benefit / invoicing / payment distribution	Not used
Sole Proprietor Account Number Routing ID	Used for benefit / invoicing / payment distribution	Not used
Sole Proprietor Account	Used for benefit / invoicing / payment distribution	Not used
Sole Proprietor Lockbox Number	Used for benefit / invoicing / payment distribution	Not used
Sole Proprietor EFT Waiver	Used for benefit / invoicing / payment distribution	Not used
Sole Proprietor Remittance Name	Used to identify individual / Sole Proprietor	Not used
Sole Proprietor Remittance Address	Used to locate individual	Not used
Sole Proprietor Remittance City	Used to locate individual	Not used

Sole Proprietor Remittance State	Used to locate individual	Not used
Sole Proprietor Zip	Used to locate individual	Not used
Sole Proprietor Country	Used to locate individual	Not used
Accounts Receivable First Name	Used to identify individual / Sole Proprietor	Not used
Accounts Receivable Last Name	Used to identify individual / Sole Proprietor	Not used
Accounts Receivable Middle Name	Used to identify individual / Sole Proprietor	Not used
Merchants ID	Used for benefit / invoicing / payment distribution	Not used
Banking account number from Vendor	EFT/ACH Used for benefit / invoicing / payment distribution	Not used
Agency banking account number	Used for benefit / invoicing / payment distribution	Not used
Electronic Funds Transfer /Automated Clearing House routing information	EFT/ACH Used for benefit / invoicing / payment distribution	Not used
Data required to process receivables and payments through the United States Treasury and financial system entities	EFT/ACH Used for benefit / invoicing / payment distribution	Not used
Insurance Information	Used for benefit /processing/ invoicing / payment distribution	Not used
Medicare Information	Used for benefit /processing/ invoicing / payment distribution	Not used
Health Insurance Information	Used for benefit /processing/ invoicing / payment distribution	Not used
Voluntary Separation Information	Used for benefit / invoicing / payment distribution	Not used
Incentive Award	Used for benefit / invoicing / payment distribution	Not used
Senior Executive Service Award	Used for benefit / invoicing / payment distribution	Not used
Travel Savings Award	Used for benefit / invoicing / payment distribution	Not used

Relocation Incentive	Used for benefit / invoicing / payment distribution	Not used
Recruitment Incentive	Used for benefit / invoicing / payment distribution	Not used
Hazard Pay	Used for benefit / invoicing / payment distribution	Not used
Student Loan Repayment	Used for benefit / invoicing / payment distribution	Not used
Supervisory Differential	Used for benefit / invoicing / payment distribution	Not used
Sole Proprietor Remittance Name	Used to identify individual / Sole Proprietor	Not used
Sole Proprietor Remittance Address	Used to locate individual	Not used
Sole Proprietor Remittance City	Used to locate individual	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?

Power BI is a third-party tool located in the Microsoft Azure government cloud to perform predictive analytics, data analysis, data, matching, relational analysis, scoring, and reporting will be utilized.

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.

FMBT Data Estate does not make available or originate data about an individual. It is sourced from IFAMS and FMS which in turn largely source their information from Treasury.

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?

In-transit: data is encrypted between the production VAEC IFAMS servers and the Data Estate's VAEC Azure Synapse. The certificate chain of trust is VA's enterprise certificate management authority and handshakes will be TLS 1.2 or 1.3.

Backups of Data Estate resources are encrypted at rest in VAEC Azure MAG.

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

The system retains Social Security Numbers as they are present in the source IFAMS database. By default: no user has access to Social Security Numbers or any other Personally Identifiable Information. They are hidden via database-level Column Level Security (CLS). Access is only granted after approval by an individual's supervisor, Data Estate officials, and the Data Estate's ISSO. Access is functionally granted by Azure Active Directory security groups.

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

The primary "product" that Data Estate offers is a scalable platform intended for reporting on financial information made available by the iFAMS software. However, just because an individual is technical in nature or has the requisite knowledge to query from this platform does not give them the authority to view or extract the potentially sensitive metadata associated to individuals. In this way, PII is safeguarded by default from querying and extract. For the protection against anticipated threats, individuals are granted privileged access on a need-to-know basis and must follow the VA's rules of conduct for continued access. The Data Estate team consists of members from the iFAMS core product team to ensure that we are providing the correct technical safeguards to ensure the security and confidentiality of records.

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 control to PII is determined by system security roles and responsibilities created in system configuration and determined and assigned by programmatic offices.

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

Access is documented via internal policy documents and stored in approved software; access is enumerated via technical means within the database system. Data Estate has performance and access monitoring tools connecting to the system to manage and track security anomalies. Data Estate data is covered under the notice 13VA047, Individuals Submitting Invoices-Vouchers for Payment and Accounting Transactional Data. Its system of records comprises of financial, accounting, benefit and, transactional data across the VA enterprise nationwide. Use case constitutes VA meeting financial management objectives for veterans, veteran health providers, and dependents.

2.4c Does access require manager approval?

Through the assigned security roles individuals will only have access to information that they have been designated "need to know." Additionally, programmatic offices/administrations/ facilities will only have access to their assigned locations and other locations are segregated by firewall configuration. These safeguards are in place to control access.

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

Through the assigned security roles individuals will only have access to information that they have been designated "need to know." Additionally, programmatic offices/administrations/ facilities will only have access to their assigned locations and other locations are segregated by firewall configuration. These safeguards are in place to control access. Data access activity logs are configured via VAEC/Azure and made available to enterprise logging systems.

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

Information Security Officer (ISO)

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

*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

•Names of recipients
•Email address
•Mailing address
•Banking account number EFT/ACH routing information from individual
•Financial account information
•Credit Card Numbers,
•Taxpayer Identification Number (TIN)
•Social security numbers/Tax ID of government employees,
•Credit card numbers
•Internet IP Addresses
•Sole proprietorship first name
•Last name
•Middle name
•Tax ID number
•Financial Institute
•Account number ABA Routing ID
•Account
•Lockbox number
•EFT Waiver
•Remittance Name
•Remittance Address
•Remittance City
•Remittance State
•Remittance Zip
•Remittance Country
•Accounts Receivable First Name
•Accounts Receivable Last Name
•Accounts Receivable Middle Name
•Merchant ID
•SSN
•Stub Name
•Retirement Indicator
•Retirement
•OASDI or Social Security
•Life Insurance
•Medicare
•Health Insurance
•Voluntary Separation Incentive Award
•Incentive Award
•Senior Executive Service Award
•Travel Savings Award
•Relocation Incentive
•Recruitment Incentive
•Retention Incentive

•Hazard Pay
•Student Loan Repayment Incentive
•Supervisory Differential

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.*

Data Estate data will be archived until it meets the disposition date documented in the records control schedule, 10-1 VHA RCS. Data will be tagged in accordance with the above RCS and move through warm to cold storage until its final disposition. Records Control Schedule 10-1 (va.gov). Information is maintained at a minimum of 6 years. Financial obligation records may be stored for 30 years as required to report on long-term loans and leases.

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

DAA-0015-2017-00

daa-0015-2017-0002_sf115.pdf (archives.gov)

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

PII maintained in Data Estate has a data retention period notated in the Finance records control schedule, MP-4, Part X Change 2, dated May 26, 1982. Also, 10-1 VHA RCS contains retention and disposition requirements for Office of Finance records which have been authorized by NARA or have been assigned a General Record Schedule (GRS) disposal authority. The VHA RCS 10-1, until MP-4, Part X Change 2 is revised, is the main authority for the retention and disposition requirements of Office of Finance records. It provides a brief description of the records, states the retention period and disposition requirements.

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.

In accordance with VA Directive 6371 Destruction of Temporary Records, it is VA policy that all Federal records contained on paper, electronic, or other medium are properly managed from their creation through their final disposition, in accordance with Federal laws, the GRS and VHA Records Control Schedule (RCS) 10-1. GRS can be found at www.archives.gov. VA Directive 6300, Records and Information Management contains the policies and responsibilities for VA's Records and Information Management program. VA Handbook 6300.1, "Records Management Procedures", Section 3.2, contains mandatory procedures for the proper management of eliminating data at the end of the retention period. Procedures are enforced by Records Management Staff and VA Records Officers. Additionally, Data Estate will comply with VA Directive 6500 Control DM-2 VA will retain PII and/or PHI for the minimum amount of time to fulfill the purpose(s)identified in the notice or as required by law; Dispose of, destroy, erase, and/or anonymize the PII and/or PHI, regardless of the method of storage in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and Use approved records disposition schedules to ensure secure deletion or destruction of PII and/or PHI (including originals, copies, and archived records). Program officials coordinate with records officers and with NARA to identify appropriate retention periods and disposal methods.

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.

Financial Management Business Transformation (FMBT) has developed programmatic policies that discuss minimalization of PII within test data. Privacy and Security training was developed and conducted on May 21, 2018, that discussed the use of Mock data when appropriate and only using live data within an accredited site. Additional, reminders have been sent through mass emails to the project personnel including contractor and government staff that reiterate the importance of using deidentified and/or mock data to test within non- accredited site. All FMBT program activities e.g., analysis, testing, UAT, etc. (except for 'go live' production migration) shall use data that has been masked or processed into synthetic data to safeguard PII sensitive data. All FMBT requests to system owners for data examples, test data, etc. shall explicitly specify the data to be provided by the request recipient has been appropriately masked prior to transfer to the requestor. In cases where system owners, representatives, etc. are unable or data volume considerations make it unapproachable to perform masking of sample and/or test data, the data cleansing/ETL team shall be engaged for assistance before the data is transferred. All sensitive data transferred for subsequent masking by the data cleansing/ETL team shall be encrypted in transit.

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: If information maintained by Data Estate is 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: To mitigate the risk posed by information retention, the Data Estate adheres to the VA RCS schedules for each category or data it maintains. When the retention data is reached for a record, the medical center will carefully dispose of the data by the determined method as described in question 3.4. VA Handbook 6500.2, "Management of Data Breaches Involving Sensitive Personal Information (SPI)" contains the policies and responsibilities that VA components are required to follow to manage data breaches, including detection, correlation, notification, remediation, and reporting.

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***
Office of Financial Services (FSC)	Human Resources – Payroll Application Services (HR-PAS). HR-PAS information cross-references IFAMS and FMS information for payment info	SSN, Stub Name, Retirement Indicator, Retirement, Social Security, Life Insurance, Medicare, Health Insurance, Voluntary Separation Incentive Award, Incentive Award, Senior Executive Service Award, Travel Savings Award, Relocation Incentive, Recruitment Incentive, Hazard Pay, student Loan Repayment, Supervisory Differential	Secure File Transfer Protocol Server (SFTP)
Office of Finance/ Financial Management Services (FMS)	FMS is the legacy system of iFAMS. FMS information may cross-reference to HR-PAS information and IFAMS information as needed to support ongoing financial	Name, SSN(s), email address, mailing address, financial account information, banking account number from individual, banking account number from Vendor, Agency banking account number, Electronic	SFTP Server

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*
	management operations.	Funds Transfer /Automated Clearing House routing information, Credit Card Numbers, Taxpayer Identification Number (TIN), and data required to process receivables and payments through the United States Treasury and financial system entities.	
FSC/ Charge Card System (CCS)	CCS is an interfacing financial system that provides Charge Card information needed to support ongoing financial management operations.	User ID Title User ID Vendor Address Code Vendor Code	Webservices
FSC/ Financial Report System (FRS)	FRS is an interfacing ad-hoc SQL reporting tool that is used to extract data from the Financial Management System FMS for reconciliation of general journal transactions relating to spending from budget & obligation through Treasury confirmation of payment.; 2. Monthly extract of accounting string level trial balances.; 3. Current Statement of Allow	Vendor Code Vendor Address Code Vendor Name User ID	SFTP server
FSC/ Invoice Payment Processing System (IPPS)	IPPS is an interfacing financial system that provides Invoice and Payment Processing	Vendor Name	SFTP server

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*
	information as needed to support ongoing financial management operations		
IFAMS/Momentum Financials	IFAMS / Momentum Financials is the next-generation of financial management software at the VA, effectively replacing FMS.	Names of recipients • Email address • Mailing address • Banking account number electronic funds transfer/Automated Clearing House (EFT/ACH) routing information from individual • Financial account information • Credit Card Numbers, • Taxpayer Identification Number (TIN) • Social security numbers/Tax ID • Credit card numbers Internet IP Addresses • Retirement Information • Insurance Information • Medicare Information • Health Insurance Information • Voluntary Separation Information • Incentive Award • Senior Executive Service Award • Travel Savings Award • Relocation Incentive • Recruitment Incentive • Hazard Pay • Student Loan Repayment • Supervisory Differential • Vendor ID • Sole proprietorship first name • Last name • Middle name • Tax ID number • Financial Institute • Account number ABA Routing ID • Account • Lockbox number • EFT Waiver Remittance Name • Remittance Address • Remittance City • Remittance State • Remittance Zip •	HTTPS

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		Remittance Country • Accounts Receivable First Name • Accounts Receivable Last Name • Accounts Receivable Middle Name • Merchant ID	

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: There is a risk that information may be shared with unauthorized VA program or system or that data could be shared.

Mitigation: Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity. Agency implementation and use of two factor authentication, encryption, built in firewalls, user access according to granted permissions, and access authorization.

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***
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: FMBT Data Estate does no sharing of data external to VA organizations. In general, the privacy risk is specific to institutional financial information for businesses and individuals.

Mitigation: Access controls are fully implemented in FMBT Data Estate resources with explicit grant permissions across all resources. Access controls are also established in the systems that source privacy information and send data to Data Estate.

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.

SORN notice 13VA047, Individuals Submitting Invoices-Vouchers for Payment and Accounting Transactional Data provides notice of information and data use of information. This SORN is review by OMB and is seeking escalation by VA Privacy Service. SORN package documents are within the appendix of this document.

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

FMBT Data Estate does not directly provide notice and/or permission to collect and disseminate. This models collection from the legacy financial system, FMS, where information is collected from other VA applications and the Department of Treasury, instead of directly from veterans, members of the public, or other individuals. As such, the system does not need to provide individuals with direct notice that it is collecting and using their information. It is assumed that these applications do provide direct notice to individuals prior to collecting information from them.

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.

While notice is not provided directly to individuals that have records stored in Data Estate, this PIA does serve as notice of the Data Estate's existence and its PII collection, use, maintenance and dissemination practices

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.

Data Estate does not collect directly from the individual. There is no ability for an individual to decline to provide information.

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.

Data Estate does not collect directly from the individual. There is no ability for an individual to decline to provide information.

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

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:

<u>Principle of Transparency:</u> Has sufficient notice been provided to the individual?

<u>Principle of Use Limitation:</u> 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 individuals who provide information to the VA interfacing application will not know how their information is being shared and used internally to the Department of Veterans Affairs

Mitigation: PIA and SORN corresponding to the legacy system FMS for which Data Estate will comply with serves as a notification for use.

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.***

SORN notice 13VA047, Individuals Submitting Invoices-Vouchers for Payment and Accounting Transactional Data, details the processes and procedures behind requesting and retrieving Privacy Act covered records. An individual wanting notification or access, including contesting the record, should mail or deliver a request to the office identified in the SORN. If an individual does not know the "office concerned," the request may be addressed to the following with below requirements: PO or FOIA/PO of any VA field station or the Department of Veterans Affairs Central Office, 810 Vermont Avenue, NW, Washington, DC 20420. The receiving office must promptly forward the mail request received to the office of jurisdiction clearly identifying it as "Privacy Act Request," and notify the requester of the referral. Approved VA authorization forms may be provided to individuals for use.

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

N/A as this system 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?

N/A as this system 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.

SORN notice 13VA047, Individuals Submitting Invoices-Vouchers for Payment and Accounting Transactional Data, details the processes and procedures behind correcting and contesting inaccurate or erroneous information. An individual may request amendment of a record pertaining to him or her contained in a specific VA system of records by mailing or delivering the request to the office concerned. The request must be in writing and must conform to the following requirements: It must state the nature of the information in the record the individual believes to be inaccurate, irrelevant, untimely, or incomplete; why the record should be changed; and the amendment desired. The requester must be advised of the title and address of the VA official who can assist in preparing the request to amend the record if assistance is desired. Not later than business 10 days after the date of a request to amend a record, the VA official concerned will acknowledge in writing such receipt. If a determination for correction or amendment has not been made, the acknowledgement will inform the individual of when to expect information regarding the action taken on the request. VA will complete a review of the request to amend or correct a record within 30 business days of the date of receipt.

Where VA agrees with the individual's request to amend his or her record(s), the requirements of 5 U.S.C. § 552a(d) will be followed. The record(s) will be corrected promptly, and the individual will be advised promptly of the correction.

If the record has previously been disclosed to any person or agency, and an accounting of the disclosure was made, prior recipients of the record will be informed of the correction. An approved VA notification of amendment form letter may be used for this purpose.

An individual wanting notification or access, including contesting the record, should mail or deliver a request to the Privacy Office or FOIA/Privacy Office of any VA field station or the Department of Veterans Affairs Central Office, 810 Vermont Avenue, NW, Washington, DC 20420.

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.

SORN notice 13VA047, Individuals Submitting Invoices-Vouchers for Payment and Accounting Transactional Data, details the processes and procedures behind correcting and contesting inaccurate or erroneous information. An individual may request amendment of a record pertaining to him or her contained in a specific VA system of records by mailing or delivering the request to the office concerned. NOTIFICATION PROCEDURES: Notification for correcting the information will be accomplished by informing the individual to whom the record pertains by mail. The individual making the amendment must be advised in writing that the record has been amended and provided with a copy of the amended record. System Manager for the concerned VA system of records, Privacy Officer, or their designee, will notify the relevant persons or organizations who had

previously received the record about the amendment. If 38 U.S.C. § 7332-protected information was amended, the individual must provide written authorization to allow the sharing of the amendment with relevant persons or organizations request to amend a record must be acknowledged in writing within 10 workdays of receipt. If a determination has not been made within this time period, the System Manager for the concerned VA system of records or designee, and/or the facility Privacy Officer, or designee, must advise the individual when the facility expects to notify the individual of the action taken on the request. The review must be completed as soon as possible, in most cases within 30 workdays from receipt of the request. If the anticipated completion date indicated in the acknowledgment cannot be met, the individual must be advised, in writing, of the reasons for the delay and the date action is expected to be completed. The delay may not exceed 90 calendar days from receipt of the request.

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.

If the individual discovers that incorrect information was provided during intake, they simply follow the same contact procedures as before, and state that the documentation they are now providing supersedes that previously provided.

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: Because there is no direct way for individuals to review or correct their information within Data Estate, there is a risk that the system may use inaccurate data when creating reports.

Mitigation: Because Data Estate ingests but does not originate the data it provides in reports, any upstream corrections to managed and unmanaged user records will flow into Data Estate, representing the correction made.

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?

An individual is provided access to the system by their system administrator within their organization.

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?

Each organization has their own criteria; however, access control to PII is determined by system security roles and responsibilities created in system configuration and determined and assigned by programmatic offices. Through the assigned security roles individuals will only have access to information that they have been designated "need to know."

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.

Each organization has their own criteria; however, access control to PII is determined by system security roles and responsibilities created in system configuration and determined and assigned by programmatic offices. Through the assigned security roles individuals will only have access to information that they have been designated "need to know." Additionally, programmatic offices/administrations/ facilities will only have access to their assigned locations and other locations are segregated by firewall configuration. These safeguards are in place to control access. Additionally, Data Estate has performance monitoring tools connecting to the system to manage and track security anomalies. IFAMs data is covered under the notice 13VA047, Individuals Submitting Invoices-Vouchers for Payment and Accounting Transactional Data. Its system of records comprises of financial, accounting, benefit and, transactional data across the VA enterprise nationwide. Use case constitutes VA meeting financial management objectives for veterans, veteran health providers, and dependents.

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.

Yes, contractors will have access to the information within Data Estate and through the contracting process, contractors are required to sign non-disclosure agreements. Contractors are working on the engineering, architecture, configuration, management of the environment, and will monitor the system for performance and security anomalies. Contractors are required to have corresponding clearances at the level and access appropriate. Contractors need to access PII is determined by the business need and the need to know. Contractors will be granted access to Data Estate if their VA manager and Privacy Officer approve. A contracting systems engineer does not have the same level or access to data as a contracted data analyst working to study legacy system data and cleansing data.

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

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

Data Estate follow agency protocols. In accordance with VA Directives 6500 and 6502, VA personnel and/or any individual that has access to the network must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. Rules are included as part of the VA Privacy and Security Awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system.

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:* 2-April 2020
3. *The Authorization Status:* ATO
4. *The Authorization Date:* 29-April-2021
5. *The Authorization Termination Date:* 28-April-2024
6. *The Risk Review Completion Date:* 2-August-2022

7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* HIGH

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

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***

N/A

Section 9 – Technology Usage

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

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

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

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, VA Enterprise Cloud (VAEC), Microsoft Azure Government (MAG) VAEC, and this is also a Software as a Service (SAAS) System.

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.*

VA maintains all ownership rights to the data it stores in Azure/MAG cloud resources.

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 collected by the CSP and disposed of (generally) after 100 days. Account financial data is stored for up to a full fiscal year. Data extracted from the CSP such as activity

logs is owned by the government and shipped to enterprise logging warehouse for long term storage.

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.

The cloud provider is only accountable for the security controls it has been explicitly approved to manage, all other controls are implemented locally by the FSC organization or shared amongst enterprise VA systems.

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).

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: 2024.03.12 10:34:42 -05'00'

Privacy Officer, Pamela M. Smith

RONALD MURRAY

Digitally signed by RONALD MURRAY
Date: 2024.03.12 14:03:39 -05'00'

Information System Security Officer, Ronald Murray

JONATHAN LINDOW

Digitally signed by JONATHAN LINDOW
Date: 2024.04.09 12:21:17 -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