Privacy Impact Assessment for the VA IT System called:

Financial Management System (FMS)

Financial Business Operations

Veterans Affairs Central Office (VACO)

Date PIA submitted for review:

10/11/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Tonya Facemire	Tonya.Facemire@va.gov	202-632-8423
Information System Security Officer (ISSO)	Neil Cruz	Neil.cruz@va.gov	202-632-7422
Information System Owner	Kishore Vakkalanka	kishore.vakkalanka@va.gov	512-981-4802

Abstract

The abstract provides the simplest explanation for "what does the system do?" and will be published online to accompany the PIA link.

The Department of Veterans Affairs (VA) owns Financial Management System (FMS) which is hosted at the Austin Information Technology Center (AITC).

FMS is the primary repository of VA financial data. FMS categorizes spending by fiscal period, station, and account.

FMS is the single VA-wide financial management system that automates and integrates VA's accounting systems and reports financial services and information to all VA organizations.

FMS is the accounting system of record for funds control, budget execution, standard general ledger, and cost accounting. FMS is a high-revenue application with cash disbursements equaling $90 to $200 million in a daily cycle per week.

FMS processing and reporting is provided by an implementation of a customized version of American Management Systems (AMS) Federal Financial System (FFS).

FMS is a Mission Critical application that maintains accounting information, processes payments and produces financial reports. It also complies with congressional mandates and oversight agency directives. It is VA's core financial management system that interfaces internally with the IFCAP Accounts Receivable system and other subsystems such as Integrated Billing.

FMS is a VA-customized Mainframe system that automates and integrates the VA's accounting systems. It features one-time transaction processing that simultaneously posts to the general ledger and to all subsidiary ledgers and tables. Data is batch processed into FMS from interfacing systems.

FMS Accreditation Boundary includes supporting applications MINX (VASI ID 2251), FRDW (VASI ID 1278), and FRS (VASI ID 1279). The Management Information Exchange System (MINX) is a mission critical, open-system data reporting tool and Oracle database (Windows and Unix Solaris servers). It provides financial information and accounting to all VA organizations which include funds control, budget execution, standard general ledger and cost accounting.

The Financial Reporting Data Warehouse System (FRDW) is a data warehouse that has been built to hold financial audit information. It maintains an interface from FMS. FRDW maintains a reconciliation and audit trail not capable under current FMS constraints. The Financial Reports System (FRS) is a web-based online query tool for building and displaying FMS data reports. The VA implemented FMS to integrate department-wide financial management systems and comply with the requirements of the Federal Managers Financial Integrity Act (FMFIA) and OMB Circulars A-130, A-127, and A-123.

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:

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether 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.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *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?*

The Department of Veterans Affairs (VA) Financial Management System (FMS), Financial Business Operations. FMS is the primary repository of VA financial data. FMS categorizes spending by fiscal period, station, and account. FMS is the single VA-wide financial management system that automates and integrates VA's accounting systems and reports financial services and information to all VA organizations. FMS is the accounting system of record for funds control, budget execution, standard general ledger, and cost accounting. FMS is a high revenue application for Enterprise Operations (EO), with FMS cash disbursements equaling $100 to $230 million daily. FMS processing and reporting is provided by an implementation of a customized version of American Management Systems (AMS) Federal Financial System (FFS). FMS manages approximately 100000 unique veteran specific records. Financial statements are generated by an implementation of Hyperion Financial Management called Management Information Exchange (MINX). MINX is an FMS data reporting tool and Oracle database. The Financial Reports System (FRS) is a web-based online query tool that accesses the database of VA data processed by FMS. The query tool comprises multiple active server pages that retrieve FMS data and build reports for display through a web browser. FMS is operated single site, at the Austin Information Technology Center (AITC).

Rogers Software Development (RSD) – A mainframe reporting system at the AITC. FMS Reports are stored on a common database on the mainframe and can be viewed by users. The reports can be printed as needed.

The VA implemented FMS to integrate department-wide financial management systems and comply with the requirements of the Federal Managers Financial Integrity Act (FMFIA) and OMB Circulars A-130, A-127, and A-123.

VA organizations account systems. FMS complies with Congressional mandates and oversight agency directives. FMS is used to describe the entire system of gathering Treasury Department and VA/FMS data, matching deposits in batch, generating reports, and online reconciliation.
FMS stores information on approximately 2.8 million individuals.
Access to the VA Intranet is controlled by defined user roles and Active Directory login permissions. VPN TCP/IP traffic of VA data is IPSEC encrypted using AES algorithms. The following laws and regulations affect FMS:

- Federal Managers Financial Integrity Act of 1982 (FMFIA)
- OMB Circular A-123 - "Internal Control Systems"
- OMB Circular A-130 - "Management of Federal Information Resources," Appendix III, “Security of Federal Automated Information Resources”
- Federal Information Security Management Act of 2002 (FISMA) (Title III, 2002 E-Gov Act)
- OMB M-03-22, “OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
- Executive Order 13103, “Computer Software Piracy”
- Government Paperwork Elimination Act (GPEA), PL 105-277
- Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191
- Information Technology Management Reform Act of 1996 (also known Clinger-Cohen Act of 1996 (40 United States Code 1452))
- 5 U.S.C. 552a, “Privacy Act of 1974,” 5 United States Code 552a, Public Law 99-08, c. 1974.
- 5 U.S.C. 552, “Freedom of Information Act,” 5 United States Code 552, c. 1967
- 18 U.S.C. 1030 (a) (3), "Fraud and related activity in connection with computers."
- 18 U.S.C. 1001, Computer Fraud and Abuse Act of 1986.
- Electronic Communications Privacy Act of 1986, Public Law 99-08, 100 Stat. 1848.
- 17 U.S.C. 106, “Exclusive rights in copyrighted works”
- 38 U.S.C. 218, "Security and law enforcement on property under the jurisdiction of the Veterans Administration"
- 38 U.S.C. 3301, "Confidential nature of claims"
- Federal Information Processing Standards (FIPS)
    - FIPS 199, “Standards for Security Categorization of Federal Information and Information Systems”
    - FIPS 200, “Minimum Security Requirements for Federal Information and Information Systems”
    - FIPS 201, “Personal Identity Verification of Federal Employees and Contractors”
    - FIPS 140-2, “Security Requirements for Cryptographic Modules”
- SORN 13VA047 /85 FR 22788 “Individuals Submitting Invoices – Vouchers for Payment-VA”

Completion of this PIA will neither result in circumstances that require changes to business processes, nor potentially result in technology changes. This system is not undergoing any significant modification that would require an amendment, revision, or approval of the SORN. FMS is not a cloud-based application.

The sources for inter-agency and extra-agency exchange of information for VA FMS are as follows:

- Department of the Treasury (DOT) - Enterprise Security Controls (ESC)
- General Services Administration (GSA) – System for Award Management (SAM)
- NPC, Inc- FMS Tax Form 1099
- Veterans Health Administration - Personnel and Accounting Integrated Data (PAID)
- Veterans Health Administration – Central Fee (FEE)
- Office of Management – Financial Reports Management (SNW)
- Office of Finance – Financial Services Center (FSC)

The Memorandum of Understanding (MOU) between Department of Treasury/ESC, GSA/SAM, NPC Inc., and FMS documents the terms and conditions for sharing data and information resources in a secure manner. The MOU also provides details pertaining to apportionment of cost and timeline for terminating or reauthorizing the interconnection. The above information may be found in Section 1.2 of this PIA.

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.

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 Account Information
☐ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers

☐ Current Medications
☐ Previous Medical Records
☐ Race/Ethnicity
☒ Tax Identification Number
☐ Medical Record Number
☐ Gender
☐ Integration Control Number (ICN)

☒Military History/Service Connection
☐ Next of Kin
☒ Other Unique Identifying Information (list below)

Banking information, Disabilities, Criminal Record Information, Veterans Preference Information, Student Loans, Education background, Benefits Information, Savings Plan Information, Credit Card Number, Claim Number, Claim for non-VA care, Provider Name, Dates Service Rendered, Description of Service (may include diagnosis), duplicate payment information and Control Number.

PII Mapping of Components

FMS consists of 1 key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by FMS and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

Note: Due to the PIA being a public facing document, please do not include the server names in the table.

PII Mapped to Components

Database Name of the information system collecting/storing PII	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
Enterprise Server (mainframe) FMS/DB	Yes	Yes	• Name • SSN • mailing address • email address • telephone number	Information is needed by current health care providers to track or reconcile the financial	VA, ITOPS Datacenter and FMS application staff have implemented required security and

			• emergency contact information • financial account information • banking information • disabilities • criminal record information • service information • veterans preference information • student loans • education background • savings plan information • benefits information • taxpayer identification number (TIN) • credit card number • claim number • claims for non-VA care • provider name • dates service rendered • description of service (may include diagnosis) • duplicate payment information	activity for VA patients.	privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA handbook 6500, Risk management Framework for VA Information Systems.

			• control number		

1.2 What are the sources of the information in the system?

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?

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 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

The sources of information for VA are as follows:

- Department of the Treasury (DOT) - Enterprise Security Controls (ESC)
- General Services Administration (GSA) – System for Award Management (SAM)
- NPC, Inc- FMS Tax Form 1099
- Veterans Health Administration - Personnel and Accounting Integrated Data (PAID)
- Veterans Health Administration – Central Fee (FEE)
- Office of Management – Financial Reports Management (SNW)
- Office of Finance – Financial Services Center (FSC)

The Memorandum of Understanding (MOU) between Department of Treasury/ESC, GSA/SAM, NPC Inc., and FMS documents the terms and conditions for sharing data and information resources in a secure manner. The MOU also provides details pertaining to apportionment of cost and timeline for terminating or reauthorizing the interconnection.

1.3 How is the information collected?

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 technology used in the storage or transmission of information in identifiable form?

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

All information is received via electronic file transmission. Sensitive data is protected through Microsoft Outlook's data encryption techniques.

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

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.

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

FMS Service ensures that financial systems comply with government wide accounting principles and standards; and are in compliance with financial policy and automated financial exchange requirements. Internal controls over data entry and transaction processing are applied throughout the system to ensure the validity of information. Personal information is contained in the VA Workload Data Files that are required for accurate product costing. All file transfers take place using VA approved secure processes; DirectConnect, FTP, or tape. Only VA staff involved in Vendor payment or Individual payment verification processes have access to change or update PII data. Interfaces with other systems are processed via jobs that are typically executed once per day. Incoming messages are transmitted to FMS in a documented file format (dataset). These messages are then processed and applied to the FMS database by the appropriate job(s). Outgoing messages are created by execution of jobs that extract, filter, and transform the FMS data.

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

FMS data standards and internal controls are regulated within the accordance of the following:

- Federal Financial Management Improvement Act (FFMIA) of 1996 – To provide accurate, reliable, and timely financial management information to government managers.
- Office of Management and Budget (OMB) Circular A-127, Financial Management Systems Requirements – To adopt standard financial business practices to use financial management shared service providers to implement and maintain their core financial system.
- Financial Systems Integration Office's (FSIO) Core Financial Systems Requirements – To consolidate and modernize financial systems and improve quality of financial information.

Chapter 4 of the VA Financial Policies and Procedures specifies that FMS do the following:

- Underlie financial and program managers' accountability for financial results
- Provide complete, timely, consistent and reliable financial information for decision making, reports and financial statements.
- Support standardized information and electronic data exchange
- Provide reliable and useful financial information on VA operations
- Maintain a single, integrated financial management system that complies with Accounting principles and standards defined by the Federal Accounting Standards Advisory board (FASAB), OMB, and the Department of Treasury.

All Austin Information Technology Center (AITC) information systems, including FMS, enforce assigned authorizations for controlling access to the system in accordance with applicable policy. All systems that store, process, or transmit sensitive information use a properly maintained and configured version of an authentication-based access control system to ensure that the sensitive information is not improperly disclosed, modified, deleted, or rendered unavailable. A list of all users who have access (even read-only) to certain types of data is reviewed quarterly.

SORN is SORN 13VA047 / 85 FR 22788 "Individuals Submitting Invoices – Vouchers for Payment-VA"

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.

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.

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

<u>Principle of Individual Participation:</u> 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 including personal contact information, service information, benefit information and financial account information may be released to unauthorized individuals.

Mitigation: The Financial Management System adheres to information security requirements instituted by the VA Office of Information Technology (OIT). VA, ITOPS Datacenter and FMS application staff have implemented required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA handbook 6500, Risk management Framework for VA Information Systems.
All employees with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.

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 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.

VA provides care and services to each unique Veteran's need, and uses the following information to distinguish each Veteran, VA Employee and VA Contractors in a unique manner:

- Name: Used to identify the veteran and retained for employee HR/Veteran record
- Social Security Number: Used as a unique veteran identifier
- Personal Mailing Address: Used for communication and retained for Veteran record
- Personal Email Address: Used for communication and retained for Veteran record
- Personal Phone Number: Used for communication and retained for Veteran record
- Emergency Contact Information: Used for communication and retained for Veteran record
- Financial Account Information: Used to interface with the Department of Treasury
- Banking Information: Used to make payments to Veterans
- Disabilities: Used by the current health care provider to track appropriate care
- Criminal Record Information: Used to identify the Veteran and retained for Veteran record

- Service Information: Used to identify the Veteran and retained for Veteran record
-
- Veterans Preference Information: Used to identify the Veteran and retained for Veteran record
- Student Loans: Used to identify the Veteran and retained for Veteran record
- record
- Education Background: Used to identify the Veteran and retained for Veteran record
- Savings Plan Information: Used to identify the Veteran and retained for Veteran record
- Benefits Information: Used to identify the Veteran and retained for Veteran record
- Taxpayer Identification Number: Used to interface with the Internal Revenue Service (IRS)
- Credit Card Number: Used to properly track payments
- Claim number: Used by current health care provider to track the financial activity
- Provider name: Used by current health care provider to track the financial activity
- Dates Service Rendered: Used by current health care provider to track the financial activity Description of Service (may include diagnosis): Used by the current health care provider to track the financial activity
- Duplicate Payment Information: Used by current health care provider to track the financial activity
- Claims for non-VA care
- Control number: Used by current health care provider to track the financial activity

This data is collected from a VA-wide financial information classification structure, the VA and from VA Medical Centers. It is also collected from the following external agency: Department of the Treasury. This information is needed to properly identify Veterans when interfacing with them. It is also needed for FMS users to identify Veterans.

2.2 What types of tools are used to analyze data and what type of data may be produced?

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.

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.
This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

FMS uses the following to analyze data:

- Financial Reports Management (SNW) – a web-based online tool used for searching and browsing reports.
- Financial Reports System (FRS) – a web-based online ad-hoc query tool that accesses a database of VA data.
- Rogers Software Development (RSD) – a computer access method used to facilitate batch and online data access.

FMS is used in support of the AITC mission, which is to provide cost-efficient IT enterprise solutions to support the information technology needs of customers within the Federal sector. Customers can view reports more efficiently than they can view the RSD mainframe reports, and these search features in FMS are very helpful for analyzing the data.

2.3 How is the information in the system secured?

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

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

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

This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest

Per the Storage Administrator, all SAN storage at data centers is encrypted. Therefore, as all servers for the system are virtual and reside on the SAN storage, all information at rest is encrypted.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

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.

VA Directive 6500 requires mandatory periodic training in computer security awareness and accepted computer security practices for all VA employees, contractors, and all other users of VA sensitive information and VA information systems. Security training is required annually for all AITC employees and VA customers who maintain or use FMS. Manager approval is required to access PII data thru the VA 9957 access process.

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

1. Name
2. Social Security Number
3. Personal Mailing Address
4. Personal Email Address
5. Telephone Number
6. Emergency Contact Information
7. Financial Account Information
8. Banking Information
9. Disabilities
10. Criminal Record Information
11. Service Information
12. Veterans Preference Information
13. Student Loans
14. Education Background
15. Savings Plan Information
16. Benefits Information
17. Taxpayer Identification Number
18. Credit Card Number
19. Claim number
20. Claims for non-VA care
21. Provider name
22. Dates service rendered
23. Description of service (may include diagnosis)
24. Duplicate Payment Information
25. Control number

3.2 How long is information retained?

In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.
This question is related to privacy control DM-2, Data Retention and Disposal.

Data is retained online for all active VA employees via reporting tools. The data is archived on tape, transferred to a records facility for three or more years, and disposed of in accordance with disposition authorization approved by the Archivist of the United States. The disposition instructions for the data records follow guidance per GRS 3.1 – Data Administration Records. This information is pending review and confirmation from the Records Management Office, information will be updated as necessary.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

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.
This question is related to privacy control DM-2, Data Retention and Disposal.

FMS records are retained within the rules of the General Records Schedule (GRS), ERA Number DAA-GRS-2013-0005 https://www.archives.gov/files/records-mgmt/rcs/schedules/general-records-schedules/daa-grs-2013-0005_sf115.pdf Records contained in the VA FMS system will be retained as long as the information is needed in accordance with a NARA approved retention period.

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the 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

Under the jurisdiction of VHA, 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. The 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. This information is pending review and confirmation from the Records Management Office, information will be updated as necessary.

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. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?
This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

FMS data is sometimes used in testing environment, PII data is protected. For Mainframe applications like FMS, CA Top Secret offers security protection for all required Started Tasks (STC) definitions and STCs that reference sensitive data or affect system integrity. The mainframe does not offer lesser mainframe protection for data as PII in all environments and/or networks as well as all applications are treated the same and fully protected.

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.

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 FMS could 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: To mitigate the risk posed by information retention, the FMS 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***
Veterans Health Administration - PAID	To provide VA Customer with generated reports for Financial data.	Name, SSN, financial account information. .	Incoming data is transmitted in a documented file format (dataset). It is then processed and applied to the database by the appropriate job(s). Outgoing data is then sent to PAID, FEE and SNW by execution of jobs that extract, filter and transform the data.
Veterans Health Administration – Central Fee (FEE)	To provide VA Customer with generated reports for Financial data.	Name, SSN, mailing address, financial account information, claims for non-VA care and duplicate payment information.	Incoming data is transmitted in a documented file format (dataset). It is then processed and applied to the database by the appropriate job(s). Outgoing data is then sent to PAID, FEE and FRM by execution of jobs that extract, filter and transform the data.
Office of Management - Financial Reports Management (SNW)	To provide VA Customer with generated reports for Financial data.	Name, SSN, mailing address, taxpayer identification number (TIN)	Incoming data is transmitted in a documented file format (dataset). It is then processed and applied to the database by the appropriate job(s). Outgoing data is

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***
			then sent to PAID, FEE and FRM by execution of jobs that extract, filter, and transform the data.
Office of Finance - Financial Services Center (FSC)	To provide VA Customer with generated reports for Financial data.	Explanations of Benefits (EOB) contains Veteran name, mailing address, claim number, provider name, dates service rendered, description of service (may include diagnosis), and control number.	Secure File Transfer Protocol (SFTP)

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.
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. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized within the facilities.

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***
Department of the Treasury Financial Management Service (DOT/FMS)/ESC	The exchange of data between the DOT/FMS and VA/FMS	Federal financial and Personally Identifiable Information (PII), such as Social Security number and Taxpayer Identification number	Interconnection Security Agreement/ Memorandum Of Understanding (ISA/MOU) signed	VPN TCP/IP traffic to the Fiscal Service is IPSEC encrypted using AES

	is for the purposes of reducing government operating costs, providing greater functionality, and improving efficiency			algorithms. Direct Connect
General Services Administration (GSA) – System for Award Management	The exchange of data between GSA and VA is for the purposes of complying with the federal mandate that vendors who wish to transact business with Federal agencies must be registered with GSA.	DUNS number, Vendor/SSN number, physical address, email address, banking information	Interconnection Security Agreement/ Memorandum Of Understanding (ISA/MOU) signed	Tectia Software – SFTP Secure File Transfer
NPC, Inc. - SFTP server	For processing data from various applications.	Federal financial and Personally Identifiable Information (PII)	Interconnection Security Agreement/Memorandum Of Understanding (ISA/MOU) signed	One-way connection using Secure File Transfer Protocol (SFTP) over a Virtual Private

				network (VPN)

5.2 **<u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>**

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.

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:
<u>Privacy Risk:</u> There is a risk that the data could be shared with an inappropriate and/or unauthorized external organization or institution.

<u>Mitigation:</u> The potential harm is mitigated by access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance.

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 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?

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. If notice was provided in the Federal Register, provide the citation.

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

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. This question is 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.

The FMS system collects information 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 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. Additionally, while notice is not provided directly to individuals that the FMS system is using their data contained in other VA IT systems, this PIA does serve as notice of the system's existence and its PII collection, use, maintenance, and dissemination practices. This PIA is available online for public notification, review, and use, as required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii). http://www.oprm.va.gov/privacy/pia.aspx. SORN is SORN 13VA047 / 85 FR 22788 "Individuals Submitting Invoices – Vouchers for Payment-VA"

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

Individuals' ability to decline to provide information is based on the needs and practices of the originating VA IT systems. Please review the PIAs and applicable SORNs for these systems to learn more. Individuals do not have the opportunity to decline to provide information to FMS because information is not collected directly from them.

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

VHA Handbook 1605.1 Appendix D 'Privacy and Release Information', section 5 lists the rights of the Veterans to request VHA to restrict the uses and/or disclosures of the individual's individually-identifiable health information to carry out treatment, payment, or health care operations. The request must be in writing Version Date: October 1, 2017 Page 18 of 29 and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record.

Individuals may have the right to consent to particular uses of the information as collected and used by the originating VA IT systems, please review the applicable PIAs and SORNs to learn more. However, individuals are not given the opportunity to consent to their information being used by FMS, as the system is used to create and view financial reports used by the VA to carry out its mandated duties.

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.

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 individuals who provide information to the VA applications FEE, FMS, and PAID will not know how their information is being shared and used internal to the Department of Veterans Affairs and will be unaware that the VA is using Financial Reports Management to create reports about VA financial and HR issues.

Mitigation: This PIA serves to notify individuals of the Financial Reports Management system and includes information about the collection of information from these systems (see questions 1.2, 1.3, and all of Section 6). Additionally, as the Financial Reports Management system is a new system, the PIAs FEE, FMS, and PAID will be updated to properly reflect the change in information sharing to add Financial Reports Management as an internal sharing partner.

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?

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.

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).

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.
This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

Individuals wishing to obtain more information about access, redress and record correction of FMS system should contact the Department of Veteran's Affairs regional as directed in the System of record Notice (SORN) Individuals Submitting Invoices-Vouchers for Payment-VA 13VA047. The SORN can be found online at:
https://www.va.gov/privacy/SystemsOfRecords/2001_Privacy_Act_GPO_SOR_compilation.pdf

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

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

Individuals wishing to obtain more information about access, redress and record correction of FMS system should contact the Department of Veteran's Affairs regional as directed in the System of record Notice (SORN) Individuals Submitting Invoices-Vouchers for Payment-VA 13VA047. The SORN can be found online at:
https://www.va.gov/privacy/SystemsOfRecords/2001_Privacy_Act_GPO_SOR_compilation.pdf

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 obtain more information about access, redress and record correction of FMS system should contact the Department of Veteran's Affairs regional as directed in the System of record Notice (SORN) Individuals Submitting Invoices-Vouchers for Payment-VA 13VA047. The SORN can be found online at:
https://www.va.gov/privacy/SystemsOfRecords/2001_Privacy_Act_GPO_SOR_compilation.pdf

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.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.

FMS is not the official record of any SPI information. 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. Formal redress procedures are published in SORN 13VA047. Individuals seeking information regarding access to and contesting of VA FMS records may write, call or visit the last VA facility where medical care was authorized or 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.

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

<u>Principle of Individual Participation:</u> 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?

<u>Principle of Individual Participation:</u> 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:

<u>Privacy Risk:</u> Because there is no direct way for individuals to review or correct their information in FMS, there is a risk that the system may use inaccurate data when creating reports

<u>Mitigation:</u> FMS does not directly collect the information in the FMS System. The data is pulled from other elements. As noted in Section 6.1 of this document:

" The FMS system collects information 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 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. Additionally, while notice is not provided directly to individuals that the FMS system is using their data contained in other VA IT systems, this PIA does serve as notice of the system's existence and its PII collection, use, maintenance, and dissemination practices**."

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?

Describe the process by which an individual receives access to the system.

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?

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.

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

Specific procedures to get access to FMS: Fill out VA Form 9957 electronically (not manually) and use the appropriate Functional Task Code (FTC): 104SW01 for FMS 1. Do NOT include your Social Security Number! Include the following information: User's LAN ID User's Name and Phone Number User's Station Number Concurring System Manager of Record (Approving Official) Active Directory (AD) Username Active Directory (AD) Domain Email Address 2. For FMS users, all reports are provided; the Station Numbers, VISN, and Organization are not required. 3. Have the Concurring System Manager of Record submit the 9957 through a digitally signed email to your designated CUPS POC. The Concurring System Manager of Record is usually the applicant’s supervisor. Public Key Infrastructure (PKI) digital certification of the email is required while encryption is unnecessary. Please do not encrypt the email before submitting to the CUPS POC. 4. The POC or ISO will forward the email and the attached 9957 request from the Concurring System Manager of Record to FMS REQUESTS. The forwarded email will provide an audit trail of the 9957 request.

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 can be granted access to FMS if their VA manager and ISO approve. They are required to follow the same procedures VA employees do for access, which is to submit a 9957 form as specified in section 8.1.
Contractors will also be required to sign NDA and confidentiality agreement.

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.

In accordance with AITC guidance, AITC personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the 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?

If Yes, provide:

1. The Security Plan Status-Current
2. The Security Plan Status Date-28-April 2022
3. The Authorization Status-Current
4. The Authorization Date-26-July 2022
5. The Authorization Termination Date 03-November 2023
6. The Risk Review Completion Date 21-September 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.

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).

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.

Not Applicable

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)

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Not Applicable

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.

Not Applicable

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.

Not Applicable

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).*

There is no Robotic Process Automation used in FMS system.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

ID	Privacy Controls
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
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**

ID	Privacy Controls
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.

Tonya L. Facemire 234776

Digitally signed by Tonya L. Facemire 234776
Date: 2022.11.16 09:09:22 -05'00'

Privacy Officer, Tonya Facemire

Neil F. Cruz 341838

Digitally signed by Neil F. Cruz 341838
Date: 2022.11.15 15:49:21 -05'00'

Information System Security Officer, Neil Cruz

Kishore N. Vakkalanka 660517

Digitally signed by Kishore N. Vakkalanka 660517
Date: 2022.11.15 14:28:31 -06'00'

Information System Owner, Kishore Vakkalanka

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).

http://www.oprm.va.gov/privacy/pia.aspx.

SORN is SORN 13VA047 / 85 FR 22788 “Individuals Submitting Invoices – Vouchers for Payment-VA” https://www.govinfo.gov/content/pkg/FR-2020-04-23/pdf/2020-08611.pdf