



Privacy Impact Assessment for the VA IT System called:

# Integrated Financial and Acquisition Management System (iFAMS)

## VACO

### Financial Services Center

### 844

Date PIA submitted for review:

10/10/2023

System Contacts:

*System Contacts*

|   | Name                  | E-mail                           | Phone Number |
|---|-----------------------|----------------------------------|--------------|
| Privacy Officer                               | Deea Lacey            | Deea.Lacey@va.gov                | 512-386-2246 |
| Information System<br>Security Officer (ISSO) | Rito-Anthony Brisbane | Rito-<br>Anthony.Brisbane@va.gov | 512-460-5081 |
| Information System<br>Owner                   | Jonathan Lindow       | Jonathan.lindow@va.gov           | 512-981-4871 |

## Abstract

*The abstract provides the simplest explanation for “what does the system do?”.*

Integrated Financial Management and Acquisition System (iFAMS) is a cloud-based momentum application intended to revolutionize Veterans Affairs financial reporting, accounting, and delivery of benefits to veterans and their beneficiaries as well as facility. This application is located within the VA Enterprise Cloud Service enclave and cloud service provider is Microsoft Azure Government (MAG). MAG has been certified as a FedRAMP High cloud though iFAMS is categorized as a moderate impact system based on a security risk assessment on the bearing of VA data surrounding confidentiality, integrity, and access.

iFAMS is replacing Financial Management System (FMS) a mainframe financial management system that interfaces with external and internal financial systems. iFAMS will interconnect to various systems and share data in the same manner. This modernization effort is expected to span until 2026. Currently, iFAMS has external interfaces with Department of Treasury, General Service Administration (GSA), US Bank, and Health and Human Services (HHS). iFAMS shares data internally to the following systems: 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), AAMS/eCMS, ConcurGov, PCS Travel, FSC Vendor Portal, FSC Data Depot, Frontier, MCAP-DSS, MinX, and WebLGY.

## 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?*  
Integrated Financial Acquisition Management System (iFAMS) 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?*

iFAMS intends to provide a comprehensive financial management system that enables VA to meet financial management objectives and comply with VA financial management policies and federal regulations. As this is a national system, iFAMS will span across all administrations, facilities, and offices throughout VA that provide benefits to veterans, their beneficiaries, physicians for veteran care, vendors, and VA employee payments such as travel and/or HR related activities. This application will collect data from thousands of veterans and their dependents, VA employees, VA contractors, and members of the public are collected and stored in this system.

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

Integrated Financial Acquisition Management System (iFAMS) is owned and operated by the Department of Veteran Affairs.

## 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?*

iFAMS includes over 300k unique records. Data is being collected by interfacing system Systems Award Management (SAM) through the Central Contractor Registration Connector (CCRC) which is a module of iFAMS.

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

Integrated Financial Acquisition Management System (iFAMS) is owned by Financial Service Center. iFAMS intends to provide a comprehensive financial management system that enables VA to meet financial management objectives and comply with VA financial management policies and federal regulations. As this is a national system, iFAMS will span across all administrations, facilities, and offices throughout VA that provide benefits to veterans, their beneficiaries, physicians for veteran care, vendors, and VA employee payments such as travel and/or HR related activities. This application will collect data from thousands of veterans and their dependents, VA employees, VA contractors, and members of the public are collected and stored in this system. iFAMS 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, and Vendor ID. 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.

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

iFAMS shares with various applications both externally and internally.

Data shared with Internal Organizations:

- Office of Financial Services (FSC), Human Resources – Payroll Application Services (HR-PAS)
- Office of Finance, Financial Management System (FMS)
- OFM VBAVACO (ALAC), WebLGY
- Office of Financial Services (FSC), MinX
- Managerial Cost Accounting Office (MCAO), MCAV-DSS
- Financial Accounting Services (FAS), Frontier
- Office of Financial Services (FSC), FSC Data Depot
- Office of Financial Services (FSC), FSC Vendor Portal

- Office of Financial Services (FSC), PCS Travel
- Office of Financial Services (FSC), ConcurGov
- Office of Acquisitions (OAL), AAMS/Ecms
- Office of Financial Services (FSC), Invoice Payment Processing System
- Office of Financial Services (FSC) Financial Report System (FRS)
- Office of Financial Services (FSC) Charge Card Services (CCS)
- Office of Financial Services (FSC) Financial Reporting Data Warehouse (FRDW)

Data shared with External Organizations:

- Health and Human Services – Payment Management System
- Department of Treasury
- System for Awards Management - General Services Administration
- US Bank
- mLINQS, LLC
- United States Department of Agriculture (USDA)

*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?*

VA takes 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 are more comprehensive than those used to validate less sensitive PII. Additional steps are necessary to validate PII that is obtained from sources other than individuals or the authorized representatives of individuals.

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, iFAMS has robotic 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.

### *3. Legal Authority and SORN*

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

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 31 U.S. Code 3512- Executive Agency Accounting and other Financial Management Reports and Plans; Federal Managers' Financial Integrity Act section 2 of 1982; Federal Financial Management Improvement Act of 1996; E-Government Act of 2002 title III., Federal Information Security Modernization Act (FISMA) of 2014; Clinger Cohen Act of 1996; 38 CFR part 17 17.120–17.132; OMB Circular A–123, Management's Responsibility for Internal Control.

[2023-18807.pdf \(govinfo.gov\)](#) SORN notice SORN 13VA047 / 85 FR 22788 Individuals Submitting Invoices-Vouchers for Payment-VA; 8/31/2023

- 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?*

SORN requires changes, SORN POC is aware and working the update.

#### 4. System Changes

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

The completion of this PIA should not result in circumstances that require changes to business processes. The iFAMS 7.9 platform will be upgraded to the 8.x platform after an approved authorization to operate (ATO). This will include the iFAMS production and lower-level environments. The CCB request for this major change is CR-445. The 8.x upgrade includes enhancements to update the technical architecture and technology stack. Oracle WebLogic will be replaced with Red Hat JBoss Enterprise Application Platform (EAP), Oracle Tuxedo will be replaced with Apache ActiveMQ, infrastructure and operations automation capabilities will be included, and the deployment of iFAMS servers will shift to containerized deployments.

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

The completion of this PIA will result in technology changes. The iFAMS 7.9 platform will be upgraded to the 8.x platform after an approved authorization to operate (ATO). This will include the iFAMS production and lower-level environments. The CCB request for this major change is CR-445. The 8.x upgrade includes enhancements to update the technical architecture and technology stack. Oracle WebLogic will be replaced with Red Hat JBoss Enterprise Application Platform (EAP), Oracle Tuxedo will be replaced with Apache ActiveMQ, infrastructure and operations automation capabilities will be included, and the deployment of iFAMS servers will shift to containerized deployments.

## 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:

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

Other PII/PHI data elements:

- 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

**PII Mapping of Components (Servers/Database)**

iFAMS consists of 7 key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by iFAMS 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*

| <b>Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI</b> | <b>Does this system collect PII? (Yes/No)</b> | <b>Does this system store PII? (Yes/No)</b> | <b>Type of PII (SSN, DOB, etc.)</b>   | <b>Reason for Collection/ Storage of PII</b>                                    | <b>Safeguards</b>  |
|--|---|---|---|---|--|
| Integrated Financial Acquisition Management  | Yes   | Yes   | Name, SSN(s), email address, mailing address, financial account information, banking account number | Veterans and vendors/customers that do business with Veterans Affairs sensitive | Internal database connections are designed to ensure the |

|   |     |     |   |  |   |
|---|-----|-----|---|--|---|
| System (iFAMS)<br>Production  |     |     | 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.   | information is required to execute legal required receivables and payments through the United States Treasury and financial system entities.   | security and integrity of the data stored within the database. Safeguards include authentication, access controls, encryption, audit and logging, etc.  |
| Integrated Financial Acquisition Management System (iFAMS) Production Standby | Yes | Yes | 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. | 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. | Internal database connections are designed to ensure the security and integrity of the data stored within the database. Safeguards include authentication, access controls, encryption, audit and logging, etc. |
| Financial Management Service (FMS)  | Yes | Yes | 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   | Veterans and vendors/customers that do business with Veterans Affairs sensitive information is required to execute legal required receivables and payments through   | Internal database connections are designed to ensure the security and integrity of the data stored within the database. Safeguards  |



|   |     |     |   |  |   |
|---|-----|-----|---|--|---|
|   |     |     | /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.   | the United States Treasury and financial system entities.  | include authentication, access controls, encryption, audit and logging, etc.  |
| Human Resources – Payroll Application Services (HR-PAS) | Yes | Yes | SSN<br>Stub Name<br>Retirement Indicator<br>Retirement<br>OASDI or Social Security<br>Life Insurance<br>Medicare<br>Health Insurance<br>Voluntary Separation<br>Incentive Award<br>Incentive Award<br>Senior Executive Service Award<br>Travel Savings Award<br>Relocation Incentive<br>Recruitment Incentive<br>Retention Incentive<br>Hazard Pay<br>Student Loan Rayment<br>Incentive<br>Supervisory Differential | 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. | Internal database connections are designed to ensure the security and integrity of the data stored within the database. Safeguards include authentication, access controls, encryption, audit and logging, etc. |
| Financial Reporting Data Warehouse (FRDW)               | Yes | Yes | SSN<br>Stub Name  | 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. | Internal database connections are designed to ensure the security and integrity of the data stored within the database. Safeguards include authentication, access controls, encryption,                         |

|                                   |     |     |  |  |   |
|-----------------------------------|-----|-----|--|--|---|
|                                   |     |     |  |  | audit and logging, etc.   |
| Charge Card Services (CCS)        | Yes | Yes | User ID<br>Title<br>Vendor Address Code<br>Vendor Code | 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. | Internal database connections are designed to ensure the security and integrity of the data stored within the database. Safeguards include authentication, access controls, encryption, audit and logging, etc. |
| Invoice Payment Processing System | Yes | Yes | Vendor Name  | 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. | Internal database connections are designed to ensure the security and integrity of the data stored within the database. Safeguards include authentication, access controls, encryption, audit and logging, etc. |

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

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

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

Information is provided by the individual or legal representative as part of an application for a benefit, contract or reimbursement. Data could potentially be obtained from a VA administration, facility and/or medical center; vendor for which VA is doing business; Department of Treasury; Internal Revenue Service; and other Federal entities. Also, sensitive data is shared from SAM system which is a one-way interfacing system through SMTP transfer.

*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.*

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.

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

iFAMS enables users to generate a variety of reports based on different scenarios pulling from the data (e.g., transactional, reference) that has been created by end-users in iFAMS. These reports include the following:

| iFAMS Report                          | Description  |
|---------------------------------------|--|
| Invalid Cards Report                  | The Credit Card Invalid Cards report displays a list of charges, credits, and other transactions against invalid credit cards loaded into the system through the Credit Card Statement Load process. The report has the functionality to allow loading of charges against invalid cards. The invalid cards are then added to the system, and the loaded charges are transferred to valid credit cards through a batch program. |
| Treasury Report on Receivables (TROR) | Momentum's Treasury Report On Receivables Report provides the ability to produce a printable report in the Treasury defined layout/format from within the system. The report reads from the TROR tables, which are populated when the Treasury Report On Receivables Extract Batch Process is run.   |
| Notice of Payment Due                 | The Notice of Payment Due Report generates follow-up dunning notices that are sent to vendors and designated agents who do not respond to the initial billing effort.  |
| SF-133                                | The SF-133 is required to be submitted at quarterly intervals but can additionally be submitted at monthly or yearly intervals. It is used for many purposes, including:   |

|                      |   |
|----------------------|---|
|                      | <ul style="list-style-type: none"> <li>• To fulfill the requirement set forth in law 31 U.S.C. 1511-1514 that the President review Federal expenditures at least four times a year.</li> <li>• To allow the monitoring of the status of funds that were apportioned on the SF-132 and funds that were not apportioned.</li> <li>• To provide a consistent presentation of information across programs within each agency, and across agencies. This enables program, budget, and accounting teams to communicate.</li> <li>• To provide historical reference that can be used to help prepare the President’s Budget, program operating plans, and spend-out rate estimates.</li> <li>• To provide a basis to determine obligation patterns when programs are required to operate under a continuing resolution.</li> <li>• To tie an agency’s financial statements to their budget execution.</li> </ul> |
| <p>Trial Balance</p> | <p>The Debt Account Trial Balance Report allows the user to view all debt accounts associated with specified Fund values, as well as information on documents that reference debt accounts. The report may be sorted in ascending order by the Debt Account Number, Debt Account Group Code, or Receivable Type</p>   |
| <p>GTAS</p>          | <p>The Governmentwide Treasury Account Symbol Adjusted Trial Balance System (GTAS) was created to allow agencies to electronically submit their budget execution information to Treasury through an adjusted trial balance. Momentum provides agencies with the ability to generate their GTAS submissions through a set of automated processes. Although the entire process is automated, Momentum offers a high degree of reporting flexibility through configuration of General Ledger Accounts, attributes values, and adjustments to online trial balance queries. The GTAS process also includes several online trial balance and validation edits reports to verify that valid data is being submitted in the GTAS file to the Department of the Treasury.</p>   |

Please note that iFAMS provides end-users the ability to execute a variety of other reports, but the reports listed above are the reports that are currently in-use by the VA community.

### **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 interfacing system SAM through the CCRC for which is a module of iFAMS.

*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?*

No, this would not apply as iFAMS does not collect information from the public that would require a clearance from OMB and store in iFAMS.

### **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 takes 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 are 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 are more comprehensive than those used to validate less sensitive PII. Additional steps are necessary to validate PII that is obtained from sources other than individuals or the authorized representatives of individuals.

*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?*

VA takes 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 are 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 are more comprehensive than those used to validate less sensitive PII. Additional steps are necessary to validate PII that is obtained from sources other than individuals or the authorized representatives of individuals.

### **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; and
- VA financial related policies and procedures.

### **1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information**

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

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

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

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

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

*Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?*

*This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.*

Follow the format below when entering your risk assessment:

**Privacy Risk:** Information being collected, used, stored, and disseminated is directly related to rendering payment, benefits, and accounting purposes which directly supports iFAMS. Privacy risks are surrounding the sensitivity of the information being collected, maintained, and stored. Also, 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:** iFAMS 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 iFAMS 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 |
|-------------------------------|---|--------------|
| Name of recipients            | Used to identify individual / Sole proprietor       | Used         |
| Email address                 | Used to contact individual                          | Used         |
| Mailing Address               | Used to locate individual                           | Used         |
| Bank Account Number EFT/ACH   | Used for benefit / invoicing / payment distribution | Used         |
| Financial Account Information | Used for benefit / invoicing / payment distribution | Used         |
| Credit Card Number            | Used for benefit / invoicing / payment distribution | Used         |
| TIN                           | Used for benefit / invoicing / payment distribution | Used         |
| SSN                           | Used to identify individual / Sole Proprietor       | Used         |
| Internet IP Address           | Used to identify individual / Sole Proprietor       | Used         |
| Sole Proprietor First Name    | Used to identify individual / Sole Proprietor       | Used         |
| Sole Proprietor Last Name     | Used to identify individual / Sole Proprietor       | Used         |

|   |   |      |
|---|---|------|
| Sole Proprietor Middle Name               | Used to identify individual / Sole Proprietor       | Used |
| Sole Proprietor TIN                       | Used for benefit / invoicing / payment distribution | Used |
| Sole Proprietor Financial Institute       | Used for benefit / invoicing / payment distribution | Used |
| Sole Proprietor Account Number Routing ID | Used for benefit / invoicing / payment distribution | Used |
| Sole Proprietor Account                   | Used for benefit / invoicing / payment distribution | Used |
| Sole Proprietor Lockbox Number            | Used for benefit / invoicing / payment distribution | Used |
| Sole Proprietor EFT Waiver                | Used for benefit / invoicing / payment distribution | Used |
| Sole Proprietor Remittance Name           | Used to identify individual / Sole Proprietor       | Used |
| Sole Proprietor Remittance Address        | Used to locate individual                           | Used |
| Sole Proprietor Remittance City           | Used to locate individual                           | Used |
| Sole Proprietor Remittance State          | Used to locate individual                           | Used |
| Sole Proprietor Zip                       | Used to locate individual                           | Used |
| Sole Proprietor Country                   | Used to locate individual                           | Used |
| Accounts Receivable First Name            | Used to identify individual / Sole Proprietor       | Used |
| Accounts Receivable Last Name             | Used to identify individual / Sole Proprietor       | Used |
| Accounts Receivable Middle Name           | Used to identify individual / Sole Proprietor       | Used |
| Merchants ID                              | Used for benefit / invoicing / payment distribution | 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?*



At this stage in the development of the system, there are no data analytic tools and/or business intelligence used. In future system implementations, tools 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.*

The newly derived information is applied to the existing record. There are three common use-cases outlined below:

- IFAMS updates existing records with any new information pertaining to employees, Several examples are as follows:
  - IFAMS has an integration with the FSC Vendor Portal and Central Contractor Registration Connector (CCRC) that synchronizes any updates with the existing records in IFAMS, if applicable. Specifically, if an individual exists as a vendor in IFAMS, any updates to their information's will integrate into IFAMS or be applied to their existing record manually.
  - Regarding Credit Cards, IFAMS has an integration with CCP that integrates all credit-card related to changes into IFAMS. For example, in the instances where a user has a card update, the update is sent through via this integration and applied to the existing record.
  - From an IFAMS access perspective, if an existing user were to transition to another organization within the VA, their existing IFAMS ID record is updated to remove their access to their previous organization and updated with access pertaining to the role that they support within their new organization.

## **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?*

iFAMS encrypts data at rest and data in transit. Microsoft Azure Government (MAG) Infrastructure that iFAMS leverages: This is inherited from FedRAMP JAB authorized package ID F1603087869 for Microsoft - Azure Government (High-IaaS). Communications through VAEC are inherited. Additionally, all commercial databases and applications (e.g. Oracle databases, IBM Tivoli suite, CA Product suite, etc.) conform to the mandates of FIPS 140-2 in regards to encrypting data at rest.

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

iFAMS enforces an additional layer of Security for various categories of PII, including SSN. The ability to view this information in IFAMS is restricted throughout the offices

and administrations. In the instances where a user does not have access, the SSN will appear as a combination of asterisks (e.g., \*\*\*\*\*); this concept is consistent across all categories of PII in iFAMS.

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

Per iFAMS PIA document, the organization a. Provides effective notice to the public and to individuals regarding: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII); (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary.

iFAMS encrypts data at rest and data in transit. Microsoft Azure Government (MAG) Infrastructure that iFAMS leverages: This is inherited from FedRAMP JAB authorized package ID F1603087869 for Microsoft - Azure Government (High-IaaS). Communications through VAEC are inherited. Additionally, all commercial databases and applications (e.g. Oracle databases, IBM Tivoli suite, CA Product suite, etc.) conform to the mandates of FIPS 140-2 in regards to encrypting data at rest.

**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. 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, iFAMS has robotic 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.

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

Yes

*2.4c Does access require manager approval?*

Yes

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

Yes

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

Internal database connections are designed to ensure the security and integrity of the data stored within the database. Safeguards include authentication, access controls, encryption, audit, and logging, etc.

## **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*

- 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 Number
- 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.*

The total data retention length is timeframe for iFAMS records is 6 years. iFAMS data is retained in the current application for three years after date of creation. Data will then be archived to a data lake for hot storage for two years and transferred into cold storage until it meets the disposition date documented in the records control schedule, 10-1 VHA RCS.

### **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?*

PII maintained in iFAMS 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. The actual defined period will be different depending on the specific record type. This requirement is also documented in the newly revised SORN 13VA047 Individuals Submitting Invoices-Vouchers for Payment and Accounting

[grs01-1.pdf \(archives.gov\)](#) GRS 1.1 Financial Management and Reporting Records

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

#### **POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:**

Individuals Submitting Invoices- Vouchers for Payment and Accounting Transactional Data-VA system of records is retained as defined by its NARA approved the General Records Schedule (GRS) GRS 1.1: Financial Management and Reporting Records, item 010. Unscheduled records within this System of Records are indefinitely retained within the rules GRS, ERA Number DAA-GRS-2013-0003-0001 (Financial transaction records). Per NARA practice, documentation for permanent electronic records must be transferred with the related records using the disposition authority of the related electronic records rather than the GRS disposition authority.

### **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](http://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, iFAMS 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.

Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction.

[https://www.va.gov/vapubs/search\\_action.cfm?dType=1](https://www.va.gov/vapubs/search_action.cfm?dType=1)

### **3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?**

*Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.*

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 June 15, 2020, 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. (with the exception of ‘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 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 iFAMS 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 iFAMS 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

| <b>List the Program Office or IT System information is shared/received with</b> | <b>List the purpose of the information being shared /received with the specified program office or IT system</b>  | <b>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</b>  | <b>Describe the method of transmittal</b> |
|---|---|---|---|
| Financial Management Service (FMS)  | 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 | 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), | SFTP server                               |



| <i>List the Program Office or IT System information is shared/received with</i> | <i>List the purpose of the information being shared /received with the specified program office or IT system</i>   | <i>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</i>   | <i>Describe the method of transmittal</i> |
|---|--|--|---|
|   | financial system entities.   | and data required to process receivables and payments through the United States Treasury and financial system entities.  |   |
| Human Resources – Payroll Application Services (HR-PAS)                         | 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. | SSN<br>Stub Name<br>Retirement Indicator<br>Retirement<br>OASDI or Social Security<br>Life Insurance<br>Medicare<br>Health Insurance<br>Voluntary Separation Incentive Award<br>Incentive Award<br>Senior Executive Service Award<br>Travel Savings Award<br>Relocation Incentive<br>Recruitment Incentive<br>Retention Incentive<br>Hazard Pay<br>Student Loan Rayment<br>Incentive<br>Supervisory Differential | SFTP server                               |
| OFM VBAVACO (ALAC) WebLGY   | 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. | Payment Amount<br>Payment Date<br>Payment Amount<br>Transaction Type   | Hybrid – Batch and Webservice             |

| <i>List the Program Office or IT System information is shared/received with</i> | <i>List the purpose of the information being shared /received with the specified program office or IT system</i>   | <i>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</i> | <i>Describe the method of transmittal</i> |
|---|--|--|---|
| Office of Financial Services (FSC) MinX   | 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. | Trading Partner<br>Dollar Amount<br>Fund   | Data Extract                              |
| Managerial Cost Accounting Office (MCAO) MCAP-DSS                               | 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. | Organization<br>Accounting Period  | Data Extract                              |
| Financial Accounting Services (FAS) Frontier                                    | 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. | Vendor Code<br>Vendor Type<br>Used ID<br>Accounting Period<br>Dollar Amount<br>Check Number  | Data Extract                              |

| <i>List the Program Office or IT System information is shared/received with</i> | <i>List the purpose of the information being shared /received with the specified program office or IT system</i>   | <i>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</i>   | <i>Describe the method of transmittal</i> |
|---|--|--|---|
| Office of Financial Services (FSC) FSC Data Depot                               | 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. | Vendor Remittance Address<br>Vendor Name<br>Contracting Officer Email Address<br>Contracting Officer Representative Email Address<br>Receipt Vendor Name<br>Vendor SSN<br>Tax Identification Number<br>Vendor Bank ABA/BIC<br>Bank Account Number<br>Vendor Bank Name<br>SSN | Data Extract                              |
| Financial Reporting Data Warehouse (FRDW)                                       | 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. | SSN<br>Stub Name   | SFTP server/File Splitting                |
| Charge Card Services (CCS)  | 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. | User ID<br>Title<br>Vendor Address Code<br>Vendor Code   | Webservices                               |

| <i>List the Program Office or IT System information is shared/received with</i> | <i>List the purpose of the information being shared /received with the specified program office or IT system</i>   | <i>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</i>   | <i>Describe the method of transmittal</i> |
|---|--|--|---|
| Office of Financial Services (FSC) FSC Vendor Portal                            | 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. | Vendor Remittance Address<br>Vendor Name<br>Contracting Officer Email Address<br>Contracting Officer Representative Email Address<br>Receipt Vendor Name<br>Vendor SSN<br>Tax Identification Number<br>Vendor Bank ABA/BIC<br>Bank Account Number<br>Vendor Bank Name<br>SSN | WebService                                |
| Office of Financial Services (FSC) PCS Travel                                   | 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. | Vendor Code<br>Vendor Address  | WebService                                |
| Office of Financial Services (FSC) ConcurGov                                    | 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. | Organization<br>Fund<br>Vendor Code<br>Vendor Address Code   | Hybrid – Batch and WebService             |

| <i>List the Program Office or IT System information is shared/received with</i> | <i>List the purpose of the information being shared /received with the specified program office or IT system</i>   | <i>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</i> | <i>Describe the method of transmittal</i> |
|---|--|--|---|
| Office of Acquisitions (OAL) AAMS/eCMS  | 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. | Vendor<br>Vendor Address Code<br>Email<br>Duns<br>Login ID<br>Contract Number<br>OEM Duns Number                                     | WebService                                |
| Office of Financial Services (FSC) Financial Report System (FRS)                | 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. | User ID<br>Vendor Address Code<br>Vendor Code<br>Fund Code<br>Vendor Name  | SFTP server                               |
| Invoice Payment Processing System   | 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. | Vendor Name  | SFTP server                               |

#### **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

| <b>List External Program Office or IT System information is shared/received with</b> | <b>List the purpose of information being shared / received / transmitted with the specified program office or IT system</b>  | <b>List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system</b>  | <b>List the legal authority, binding agreement , SORN routine use, etc. that permit external sharing (can be more than one)</b> | <b>List the method of transmission and the measures in place to secure data</b> |
|--|--|---|---|---|
| HHS-PMS  | Health and Human Services – Payment Management System<br><br>Integrates with iFAMS to facilitate the flow of grants funds between the Federal Government and grant recipients. | The transmitted data contains PII which includes vendor financial data (Taxpayer Identification Number [TIN]/Employer Identification Number [EIN]/Social Security Number [SSN]) without individual’s name or company name.  | ISA/MOU - 1   | SFTP (SSH File Transfer Protocol)   |
| Bureau of Fiscal Service Treasury Web Application Infrastructure                     | Department of Treasury<br><br>The data that traverses this connection contains federal financial information as well as  | The data that traverses this connection contains federal financial information as well as Privacy Act data and is classified Sensitive but Unclassified (SBU) PII data (Personally Identifiable Information: Recipient and Vendor: name, vendor id, address, banking information)). The data sensitivity classification for confidentiality is high, integrity high, and availability high. | ISA/ MOU - 3  | SFTP (SSH File Transfer Protocol)   |

|                                     |   |   |             |                                   |
|-------------------------------------|---|---|-------------|-----------------------------------|
|                                     | Privacy Act data and is classified Sensitive but Unclassified (SBU) PII                             |   |             |                                   |
| The System for Award Management SAM | Integrates with IFAMS to send registered SAM vendors  | Sole proprietorship first name<br>Last name<br>Middle name<br>Tax ID number<br>Financial Institute<br>Account number ABA Routing ID<br>Account<br>Lockbox number<br>EFT Waiver<br>Remittance Name<br>Remittance Address<br>Remittance City<br>Remittance State<br>Remittance Zip<br>Remittance Country<br>Accounts Receivable First Name<br>Accounts Receivable Last Name<br>Accounts Receivable Middle Name<br>Name<br>Merchant ID | ISA/MOU - 2 | SFTP (SSH File Transfer Protocol) |
| US Bank                             | IFAMS receives a daily statement file that contains card charges (i.e., Purchase Card, CBA, Fleet). | <b>USBconur_weekly_filelayout</b><br><br>Account number<br>Reference Number<br>Posting Date<br>Passenger Name<br>Ticket Number<br>Travel Agency Code<br>Travel Agency Name<br>Source Amount<br>Obligation<br>Passenger specific data<br><br><b>USBANK-CCS-001-PowerTrack_filelayout</b><br><br>Account number<br>Posting Date<br>Transaction Date<br>Merchant Name<br>Merchant City<br>Merchant State<br>Merchant Zip               | ISA/MOU - 1 | SFTP (SSH File Transfer Protocol) |



|                                       |  |   |             |   |
|---------------------------------------|--|---|-------------|---|
| mLINQS Hosting Service (MHS), (iMOVE) | IFAMS receives travel authorizations, travel payments, and billing documents from the iMOVE integration                    | Data transmitted from MHS to Integrated Financial, and Acquisition Management System (iFAMS) includes financial information. Taxable Travel data is entered into MHS where it is processed and stored in support of taxable relocation travel. Relevant financial data is transmitted to the VA for the purpose of recording financial transaction in the VA's financial accounting system of record. | ISA/MOU - 1 | Data is transmitted synchronously using SOAP over HTTPS from mLINQS, LLC to VA. |
| Midrange Systems and Mainframe        | United States Department of Agriculture (USDA)<br><br>Sensitive data is transmitted to the VA over this connection weekly. | Sensitive data is transmitted to the VA over this connection weekly. The data that is transmitted to VA iFAMS includes PII (Social Security Number, address, name, phone number, email) data, and Payroll financial (Salary, benefits, and Payment's data). Information shared is categorized as Controlled Unclassified Information (CUI)  | ISA/MOU - 1 | SSH FTP (Secure Shell FTP)  |

**5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure**

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

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

*Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.*

*Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.*

*This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing*

Follow the format below:

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

**Mitigation:** 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 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 under revision and has been concurred on by office of general counsel, office of congressional affairs, privacy service and ifams authorizing official. It is waiting on chief information officer approval in order to move outside the agency. Sorn package documents are within the appendix of this document. [Federal Register :: Privacy Act of 1974; System of Records](#)

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

SORN 13VA047, Individuals Submitting Invoices-Vouchers for Payment-VA [Federal Register :: Privacy Act of 1974; System of Records](#)

*6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection. The provided SORN explain the reason, purpose, authority, and routine uses of the collected information is adequate to inform those affected by the system that their information has been collected and is being used appropriately.*

System of Records Notice (SORN) is clear about the use of the information, specifically SORN: 13VA047 - Individuals Submitting Invoices-Vouchers for Payment-VA

[Federal Register :: Privacy Act of 1974; System of Records](#)

**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.*

iFAMS 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.*

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

**6.4 PRIVACY IMPACT ASSESSMENT: Notice**

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

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

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

*Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?*

*This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.*

Follow the format below:

**Privacy Risk:** There is a risk that individuals who provide information to the VA interfacing application will not know how their information is being shared and used internal to the Department of Veterans Affairs.

**Mitigation:** The VA Chief Privacy Officer (CPO) documents and ensures implementation of Privacy Continuous Monitoring (PCM) program, which maintains an ongoing awareness of threats and vulnerabilities that may pose privacy risks; monitors changes to information systems and environments of operation that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII; conducts privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented at the agency across the agency risk management tiers to ensure continued compliance with applicable privacy requirements and management of privacy risks. The CPO in conjunction with the VA Privacy Service also document and ensure implementation of enterprise-wide policy for incorporating use of Privacy Threshold Analysis (PTA) and Privacy Impact Assessment (PIA) to manage privacy risk and evaluate how information processing practices at each stage of the information "life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) may affect an individual's privacy. The Information System Owner (ISO) in conjunction with the Information System Security Officer (ISSO), Privacy Officer (PO), and Information Owner are responsible for conducting a Privacy Threshold Analysis (PTA) and Privacy Impact Assessment (PIA) following the process outlined in VA Handbook 6508.1, Procedures for Privacy Threshold Analysis and Privacy Impact Assessment.

## 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.***

VA 6300.4 Section 3. Procedures for Handling Requests for Access to or Amendment of Records. The Privacy Officer is responsible for adhering to a Privacy Act request as outlined in VA Handbook 6300.4: Procedures for Processing Requests for Records Subject to the Privacy Act. See attached VA 6300.4. The Privacy Officer is responsible for the organization adheres to OMB policies and guidance for the proper processing of Privacy Act requests.

*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)?*

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.

*7.1c 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?*

. iFAMS is not a Privacy Act system. 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.

## **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 ensure data accuracy.***

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

The iFAMS Information Owner in collaboration with Privacy Officer (PO) ensure that individuals are informed via System of Records Notice (SORN) about VA's procedures on gaining access to records pertaining to them contained in the system of records and contesting its contents. Further, the Privacy Officer who has jurisdiction over the records subject to the Privacy Act request follows established procedures for reviewing and addressing request to correct a record. The Privacy Officer acknowledges in writing receipt of a request to amend a record no later than 10 business days after the date of the request; informs the individual of when to expect information regarding the action taken on the request; completes a review of the request to amend or correct a record within 30 business days of the date of receipt; corrects the records promptly and advises individuals of such correction in accordance with applicable laws and regulations.

### **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 iFAMS, there is a risk that the system may use inaccurate data when creating reports.

**Mitigation:** iFAMS system configuration encompasses an Enterprise Service Bus that will orchestrate the migration, analysis, and cleansing of the data before it is transmitted from an interfacing system to iFAMS.

## 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. 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, iFAMS has robotic 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.

#### *8.1b 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?*

The Administration or Office Budget-Entry user will be allowed to Reviews / confirm historical data amounts during Technical Call Review (Script, Layout 1 – Technical Call Review) within the assigned Security Organization. The Administration or Office user will be allowed to Enter budget amounts for assigned VA Funds for Internal Submission (Script / Layout 3), OMB Submission (Script / Layout 5), OMB Account Allocation (Script / Layout 7), President’s Budget (Layout 8) and OMB MAX Rounding Resolution (Script / Layout 9) within the assigned Security Organization. The Administration or Office Budget-Approval user will be allowed to review and approve budget requests at three different approval levels within the assigned Security Organization. VA Office of Budget Initiator will assign Administrations / Offices / Funds, the VA Office of Budget Initiator ensures layout requests are to release for Admin / Office budget entry. For assigned Administrations / Offices / Funds, the VA Office of Budget Initiator confirms historical data import (Script / Layout B-Import). For assigned Administrations / Offices / Funds, the VA Office of Initiator enters amounts for Spring Guidance (Script / Layout 2), Secretary’s Decision (Script / Layout 4), OMB Passback (Script / Layout 6), and Congressional Action (Script / Layout 10). Office of Budget Approval assigned Administrations / Offices / Funds, the VA Office Budget-Approval user will be allowed to review and approve budget requests at three different approval levels. Budget Request Query user will have access to run Formatted Systems Queries and view the Budget Request amounts previously entered in the



formulation process within the permitted Security Organizations. Office of Budget Administrator will have access to all functionalities with all valid permissions except for Security components. iFAMS System Administrator role will have access to all functionalities with all valid permissions. System Administrator role will have access to all functionalities with all valid permissions.

*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.*

IFAMS contains a variety of roles that provide end-users with the ability to perform various actions depending on their role and the level of support that they provide for their organization(s); each role is configured to align with one of three categories:

- Miscellaneous Roles (i.e., View Only, Update tables, Generate Reports)
- Submitter/Corrector Roles (i.e., Provide users with the ability to create or correct transactions)
- Approver Roles (i.e., Provide users with the ability to approve transactions)

In IFAMS, we currently have a total of 1,686 roles.

**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 iFAMS 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 iFAMS if their VA manager and Privacy Officer approval. 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.*

iFAMS 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? Yes**

*8.4a If Yes, provide:*

- 1. The Security Plan Status: Approved*
- 2. The System Security Plan Status Date: 08/03/2023*
- 3. The Authorization Status: Authorization to Operate (ATO)*
- 4. The Authorization Date: 07/22/2021*
- 5. The Authorization Termination Date: 07/21/2024*
- 6. The Risk Review Completion Date: 07/15/2021*
- 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.*

*<<ADD ANSWER HERE>>*

## **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 (ITMAaaS). 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)

iFAMS utilizes the VA Enterprise Cloud (VAEC), Platform as a Service (PaaS). The Cloud Service Provider (CSP) is Microsoft Azure Government (MAG).

**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.*

NA

**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.*

NA

**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.*

NA

**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).*

NA

## Section 10. References

### Summary of Privacy Controls by Family

*Summary of Privacy Controls by Family*

| <b>ID</b> | <b>Privacy Controls</b>                                     |
|-----------|---|
| <b>AP</b> | <b>Authority and Purpose</b>                                |
| AP-1      | Authority to Collect  |
| AP-2      | Purpose Specification                                       |
| <b>AR</b> | <b>Accountability, Audit, and Risk Management</b>           |
| 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                                   |
| <b>DI</b> | <b>Data Quality and Integrity</b>                           |
| DI-1      | Data Quality  |
| DI-2      | Data Integrity and Data Integrity Board                     |
| <b>DM</b> | <b>Data Minimization and Retention</b>                      |
| DM-1      | Minimization of Personally Identifiable Information         |
| DM-2      | Data Retention and Disposal                                 |
| DM-3      | Minimization of PII Used in Testing, Training, and Research |
| <b>IP</b> | <b>Individual Participation and Redress</b>                 |
| IP-1      | Consent   |
| IP-2      | Individual Access   |
| IP-3      | Redress   |
| IP-4      | Complaint Management  |
| <b>SE</b> | <b>Security</b>   |
| SE-1      | Inventory of Personally Identifiable Information            |
| SE-2      | Privacy Incident Response                                   |
| <b>TR</b> | <b>Transparency</b>   |
| TR-1      | Privacy Notice  |
| TR-2      | System of Records Notices and Privacy Act Statements        |
| TR-3      | Dissemination of Privacy Program Information                |
| <b>UL</b> | <b>Use Limitation</b>                                       |
| UL-1      | Internal Use  |
| UL-2      | Information Sharing with Third Parties                      |

**Signature of Responsible Officials**

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

---

**Privacy Officer, Deea Lacey**

---

**Information Systems Security Officer, Rito-Anthony Brisbane**

---

**Information Systems 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).

[Federal Register :: Privacy Act of 1974; System of Records](#)

## **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](#)