
Privacy Impact Assessment for the VA IT System called:

# Financial Content Management (FCM)

# VACO

# Office of Service Delivery and Engineering

Date PIA submitted for review:

08/17/2022

System Contacts:

*System Contacts*

| | Name | E-mail | Phone Number |
|---|---|---|---|
| Privacy Officer | Gina Siefert | Gina .siefert@va.gov | 224-558-1584 |
| Information System Security Officer (ISSO) | Tamer Ahmed | tamer.ahmed@va.gov | 202-461-9306 |
| Information System Owner | David Larson | david.larson@va.gov | 512-534-5966 |

## Abstract

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

The purpose of the VA's Financial Content Management (FCM) product is to support Central-FEE (FEE), Financial Management System (FMS), and HR Payroll (HRPAS) applications with online report storage, indexing, archive, retrieval, management, and secure presentment. The FCM application will present the reports via secure web browser to the user who can review data pertinent to their established security profile in the application.

## Overview

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

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

The Financial Content Management (FCM) product is owned by the Office of Finance.

The completion of this PIA will not result in circumstances requiring changes to business processes.

The completion of this PIA will not result in technology changes.

FCM neither creates, collects, or shares any information for anyone identified on FEE, FMS, or HRPAS reports.

- All vendors providing goods and/or services to VA enterprise-wide display upon FMS System Reports and are available for viewing using FCM in desktop browser.
- All full-time, part-time, and fee-basis employees working at VA enterprise-wide display upon HRPAS System Reports and are available for viewing using FCM in desktop browser.
- All payments to vendors providing goods and/or services to VA enterprise-wide display upon FEE System Reports and are available for viewing using FCM in desktop browser.

The FCM product, and the FEE, FMS, and HRPAS report data are separate from one another, but both product and data are hosted at the Austin Information Technology Center (AITC).

The FCM product is a web front end bridge and provides FEE, FMS, and HRPAS only with desktop access from within VA firewalls to view their mainframe reports online. No changes are required in business as result of PIA because reports once available for viewing in FRM SnapWeb (SNW) product are now available in the FCM product.

FCM supports VA with secure online report presentment, indexing, archive, retrieval, and management. The FEE, FMS, and HRPAS systems are only a few examples currently viewing their reports online using FCM. The FEE, FMS, and HRPAS reports contain data to process human resources, payroll, and financial services. This information consists of financial data, privacy act data, and personally identifiable information (PII) data.

The FCM product will present the reports via FCM's secure web interface to the user who can review data pertinent to their established security profile in the application. The report displays in the browser is only available during an active session, once the browser is closed, the cache is cleared, and the information is no longer available via FCM.

FCM uses standard technology to meet privacy and security standards established by VA guidelines. FCM has the potential to be used by all VA employees.

All information provided to FCM comes in the form of pregenerated reports. FCM allows FEE, FMS, and HRPAS to view their reports using a web browser. Once the web browser is closed, the cache memory is cleared, and the reports are no longer available via FCM. Here is how FEE, FMS, and HRPAS use the information:

1. FEE – Provides historical records of payments made. Allows staff to construct and search a wide range of claims data, including 'potential duplicate payment' report.

2. FMS – Integrates VA's accounting systems and reports financial services and information to all VA organizations.

3. HRPAS - Produces reports needed to meet the VA payroll reporting requirements. This includes Earning and Leave statements, W2s, Defense Civilian Pay System (DCPS) interfaces, Gross-to-Net reports, retirement reporting, various accounting reports, and data updates.

The legal authority is Executive Order 9397, which allows the collection and use for business purposes/enrollment and 32 CFR 505.4(a)(b) for individual's rights, benefits, and privileges under federal programs.

SORN info for FEE, FMS, and HRPAS systems already exist, require no modification or approval because FCM product displays reports similarly to the product it's replacing; FRM SnapWeb (SNW).

FEE 23VA10NB3 - Non-VA Care (Fee) Records

FMS 13VA047 - Individuals Submitting Invoices-Vouchers For Payment

HRPAS 171VA056A/78 FR 63311 Human Resources Information

## Section 1. Characterization of the Information

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

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

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

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

*The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1.*

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

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☒ Personal Email Address
- ☒ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☒ Financial Account Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Current Medications

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

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

Disabilities
Criminal Record Information Service Information

Veteran Preferences
Student Loans Information
Education Information
Savings Plan Information
Benefit Information

FCM neither creates, collects, disseminates, or validates any information, whatsoever, for any individuals identified on FEE, FMS, or HRPAS reports. The FCM product only displays reports containing the information collected by the FEE, FMS, and HRPAS systems.

**PII Mapping of Components**

Financial Content Management (FCM) consists of no key components that collect PII. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Financial Content Management (FCM) and the reasons for the collection of the PII are in the table below.

**PII Mapped to Components**

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

*PII Mapped to Components*

| Database Name of the information system collecting/storing PII | Does this system collect PII? (Yes/No) | Does this system store PII? (Yes/No) | Type of PII (SSN, DOB, etc.) | Reason for Collection/ Storage of PII | Safeguards |
|---|---|---|---|---|---|
| N/A | No | N/A | N/A | N/A | N/A |

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

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

*Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.*

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

The FEE, FMS, and HRPAS systems maintain report content, data quality, and privacy control, as well as any/all consent for checked data identified in section 1.1 and are the system/s of record.

FCM allows FEE, FMS, or HRPAS systems' personnel only to view reports of data sourced from their own respective systems.

FCM neither creates, collects, disseminates, validates, or obtains consent for information content identified on the FEE, FMS, or HRPAS reports.

The FEE, FMS, and HRPAS systems are the sole source of information displayed by customer in FCM.

The SORN/s as follows.

FEE 23VA10NB3 - Non-VA Care (Fee) Records

FMS 13VA047 - Individuals Submitting Invoices-Vouchers For Payment

HRPAS 171VA056A/78 FR 63311 Human Resources Information

**1.3 How is the information collected?**

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

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

FCM neither creates, collects, disseminates, or validates any information, whatsoever, for any individuals identified on FEE, FMS, or HRPAS reports. The information used by FCM is collected by the FEE, FMS, and HRPAS systems.

FCM only displays the information via web browser and is available only during the active session. Once browser is closed the cache is cleared and the information no longer exists in FCM.

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

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

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

The FEE, FMS, and HRPAS systems are responsible for maintaining privacy controls, data quality, and data integrity for all data checked in section 1.1 and are the system of record.

FCM neither creates, collects, disseminates, or validates any information, whatsoever, for any individuals identified on FEE, FMS, or HRPAS systems' reports. The pre-generated reports can only be displayed via browser using FCM.

The FCM product assumes accuracy of information collected by the FEE, FMS, and HRPAS systems, and does not do any additional verification.

Any frequency for checking of information is predetermined by the FEE using FEE System Reports generated daily, weekly, monthly, quarterly, and semi-annually, FMS using FMS System Reports generated monthly, and HRPAS system using HRPAS System Reports generated bi-weekly because FCMs only purpose is to allow users to view their reports.

The SORN/s are as follows.

FEE 23VA10NB3 - Non-VA Care (Fee) Records

FMS 13VA047 - Individuals Submitting Invoices-Vouchers For Payment

HRPAS 171VA056A/78 FR 63311 Human Resources Information

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

*List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any*

*potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders.*
*This question is related to privacy control AP-1, Authority to Collect*

The legal authority is Executive Order 9397, which allows the collection and use for business purposes/enrollment and 32 CFR 505.4(a)(b) for individual's rights, benefits, and privileges under federal programs.

The SORN/s are as follows.

FEE 23VA10NB3 - Non-VA Care (Fee) Records

FMS 13VA047 - Individuals Submitting Invoices-Vouchers For Payment

HRPAS 171VA056A/78 FR 63311 Human Resources Information

## 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.*

*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.*

**Privacy Risk:**
FCM displays Personally Identifiable Information (PII). If this information is breached or accidentally released to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to the individuals whose information is contained in the system.

**Mitigation:**

- Access to FCM is through the VA network via secure web browser interface, there is no public facing interface.

- Users can only review data pertinent to their established security profile in the product.

- FCM adheres to information technology security requirements instituted by the VA Office of Information Technology (OIT).

- All employees with access to information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.

## Section 2. Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

**2.1 Describe how the information in the system will be used in support of the program's business purpose.**

*Identify and list each use (both internal and external to VA) of the information collected or maintained.*
*This question is related to privacy control AP-2, Purpose Specification.*

FCM does not collect, store, generate, or aggregate data directly from individuals. The FCM product's only use of the information is to provide a means to view the FEE, FMS, and HRPAS systems generated reports via a web browser.

The information collected by the FEE, FMS and HRPAS systems is identified as follows.

1. Benefit Information – Employee annual enrollment and payroll processing.
2. Criminal Record Information Service Information – HRPAS uses for Human Capital Management.
3. Date of Birth – used for Human Capital Management by HRPAS system.
4. Disabilities – used for Human Capital Management by HRPAS system.
5. Education Information – used for Human Capital Management by HRPAS system.
6. Emergency Contact Info – used for Human Capital Management by HRPAS system.
7. Financial Account Information – Payroll processing, Financial Management Invoice payments.
8. Name – Central-FEE, FMS, and HRPAS systems to process individuals within their own systems.
9. Personal Email Addresses - Central-FEE, FMS, and HRPAS systems use to correspond with individuals.
10. Personal Mailing Address - Central-FEE, FMS, and HRPAS systems use to correspond with individuals.

11. Personal Phone Numbers - Central-FEE, FMS, and HRPAS systems use to correspond with individuals.
12. Savings Plan Information - HRPAS system uses for payroll processing.
13. Social Security Number – Central-FEE, FMS, and HRPAS use for paychecks and/or invoice payments.
14. Student Loans - used for Human Capital Management by HRPAS system.
15. Tax Identification Number – Central-FEE and FMS use for invoice payments, etc..
16. Veteran Preferences – used for Human Capital Management by HRPAS system.

The SORN/s are as follows.

FEE 23VA10NB3 - Non-VA Care (Fee) Records

FMS 13VA047 - Individuals Submitting Invoices-Vouchers For Payment

HRPAS 171VA056A/78 FR 63311 Human Resources Information

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

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

*If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.*
*This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information*

FCM does not create or make available previously unutilized information about an individual.

**2.3 How is the information in the system secured?**

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

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

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

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

VA Directive 6500 https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=1254&FType=2 requires mandatory periodic training in computer security awareness and accepted computer security practices for all VA employees, contractors, and all other users of VA sensitive information and VA information systems. Security training is required annually for all AITC employees and VA customers who maintain use of FCM.

FCM neither creates, collects, disseminates, or validates any information, whatsoever, for any individuals identified on FEE, FMS, or HRPAS reports. The information used by FCM is collected by the FEE, FMS, and HRPAS systems.

FCM only displays the information via web browser and is available only during the active session. Once browser is closed the cache is cleared and the information no longer exists in FCM.

- FCM operates behind the VA Firewall with Virtual Private network (VPN) and smart card credentials to protect data in transit and at rest.

- FCM also establishes user profiles for authorized personnel to view encrypted data on a need-to-know basis to protect data in transit and at rest.

- FCM only displays Social Security Number when imbedded in the FEE, FMS, and/or HRPAS reports and relies upon FEE, FMS, and/or HRPAS measures in place.

The legal authority is Executive Order 9397, which allows the collection and use for business purposes/enrollment and 32 CFR 505.4(a)(b) for individual's rights, benefits, and privileges under federal programs.

The SORN/s are as follows.

FEE 23VA10NB3 - Non-VA Care (Fee) Records

FMS 13VA047 - Individuals Submitting Invoices-Vouchers For Payment

HRPAS 171VA056A/78 FR 63311 Human Resources Information

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

*Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. Example: Describe if training for users of the project*

*covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.*

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

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

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

VA Directive 6500 requires mandatory periodic training in computer security awareness and accepted computer security practices for all VA employees, contractors, and all other users of VA sensitive information and VA information systems. Security training is required annually for all AITC employees and VA customers who maintain or use FCM. Manager approval is required to access PII data thru the VA 9957 access process, and access privileges are determined by user's Job Title Role. FCM records access to FEE, FMS, and HRPAS reports, and any/all safeguards are responsibility of FEE, FMS, and/or HRPAS.

The SORN/s are as follows.

FEE 23VA10NB3 - Non-VA Care (Fee) Records

FMS 13VA047 - Individuals Submitting Invoices-Vouchers For Payment

HRPAS 171VA056A/78 FR 63311 Human Resources Information

## 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*

FCM only retains the FEE, FMS, and/or HRPAS report in the web browser's cached memory for the extent of the active session. Once the web browser is closed, the cache is cleared, and the information provided no longer exists in FCM.

**3.2 How long is information retained?**

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

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

FCM only retains the FEE, FMS, and/or HRPAS report in the web browser's cached memory for the extent of the active session. Once the web browser is closed, the cache is cleared, and the information provided no longer exists in FCM.

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

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

The disposition authority is documented in Record Control Schedule 10-1. VA Form 0751, and Information Technology Equipment Sanitization Certificate. Records contained in the VA FEE, FMS, and/or HRPAS system will be retained as long as the information is needed in accordance with a NARA-approved retention period. No records are disposed of or destroyed without the approval of the facility's Record Control Manager. All records are disposed of in accordance with VA Policy and disposition authority (RCS 10-1). Archived and retired records are maintained in accordance with VA Policy.

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf (Records Control Schedule 10-1)
www.va.gov/vapubs/viewPublication.asp?Pub_ID=20&FType=2 (VA Handbook 6300)
http://vaww.va.gov/vaforms/va/pdf/VA0751(ES).pdf (VA Form 0751)

**3.4 What are the procedures for the elimination of SPI?**

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

Under the jurisdiction of VHA, it is VA policy that all Federal records contained on paper, electronic, or other medium are properly managed from their creation through their final disposition, in accordance with Federal laws, the General Records Schedule (GRS) and VHA Records Control Schedule (RCS) 10-1. The GRS can be found at www.archives.gov. VA Directive 6300, Records and Information Management contains the policies and responsibilities for VA's Records and Information Management program. VA Handbook 6300.1, "Records Management Procedures", Section 3.2, contains mandatory procedures for the proper management of eliminating data at the end of the retention period. Procedures are enforced by Records Management Staff and VA Records Officers. Paper documents may be shredded or burned and record destruction is documented in accordance with NARA guidelines. Selected destruction methods for other data media comply with NCSC-TG-025 Version-2/VA Policy. Other IT equipment and electronic storage media are sanitized in accordance with procedures of the NSA/Central Security Service Media Declassification and Destruction Manual and certified that the data has been removed or that it is unreadable. Certification identifies the Federal Information Processing (FIP) item cleared. FIP equipment is not excessed, transferred, discontinued from rental or lease, exchanged, or sold without certification. The disposition authority is documented in Record Control Schedule 10-1, Section XLIII-1 and XLIII-2. Disposition instructions and procedures for electronic media are documented in NCSC-TG-025 Version2/VA Policy, VA Form 0751, and Information Technology Equipment Sanitization Certificate. No records are disposed/destroyed without the approval of the facility's Record Control Manager. All records are disposed of in accordance with VA Policy and disposition authority (RCS 10-1). Archived and retired records are maintained in accordance with VA Policy.

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

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

The FCM product uses existing mainframe system security features to enable customers to view select reports online. All authorized customers' viewing reports are VA employees or VA contractors and complete training annually for security roles and rules of behavior.

**3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>**

*Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.*

*While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of*

*PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.*

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

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

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

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

**Mitigation:** To mitigate the risk posed by information retention, FCM adheres to the NARA General Records Schedule. When the retention date is reached for a record, the individual's information is carefully disposed of by the determined method as described in General Records Schedule 10-1

## Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

*Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?*

*This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.*

*Data Shared with Internal Organizations*

| ***List the Program Office or IT System information is shared/received with*** | ***List the purpose of the information being shared /received with the specified program office or IT system*** | ***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*** | ***Describe the method of transmittal*** |
|---|---|---|---|
| Central-FEE | To let customers in Central-FEE, view their generated reports. | Name<br>Personal Email Address<br>Personal Mailing Address<br>Personal Phone<br>Social Security Number<br>Tax Identification Number | Nothing transmitted! Reports created by Central-FEE are displayed via FCM secure web interface. |
| Financial Management System (FMS) | To let customers in FMS, view their generated reports. | Name<br>Financial Account Information<br>Personal Email Address<br>Personal Mailing Address<br>Personal Phone<br>Social Security Number<br>Tax Identification Number | Nothing transmitted! FCM displays reports created by FMS via FCM secure web interface. |
| Human Resources and Payroll Application Services (HRPAS) | To let customers in HRPAS, view their generated reports. | Benefit Information<br>Criminal Record Information<br>Service Information<br>Disability<br>Education Information<br>Emergency Contact Info<br>Financial Account Information<br>Date of Birth<br>Name<br>Personal Email Address<br>Personal Mailing Address<br>Personal Phone<br>Savings Plan Info<br>Social Security Number<br>Student Loans<br>Tax Identification Number<br>Veteran Preferences | Nothing transmitted! FCM displays reports created by FMS via FCM secure web interface. |

## 4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

*Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks.*
*This question is related to privacy control UL-1, Internal Use.*

**Privacy Risk:** The privacy risk associate with maintaining PII is that sharing data within the Department of Veterans' Affairs could happen and that the data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

**Mitigation** Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized within the facilities.

## Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

*Data Shared with External Organizations*

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

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M06-16, note them here.

N/A

## 5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

*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*

**Privacy Risk:** The privacy risk associated with maintaining PII is that sharing data outside of the Department of Veteran's Affairs could happen, and that data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

**Mitigation:** Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized within the facilities.

## Section 6. Notice

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

**6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?**

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

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

*Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection. This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.*

FCM does not directly collect the information displayed in the system. The information is pulled from other VA systems (FEE, FMS, HRPAS). Any notice provided would be made through those applications.

FEE SORN Link - 23VA10NB3 - Non-VA Care (Fee) Records

FMS SORN Link - 13VA047 - Individuals Submitting Invoices-Vouchers For Payment

HRPAS SORN Link - 171VA056A/78 FR 63311 Human Resources Information

Additionally, while notice is not provided directly to individuals that the Financial Reports Management (SNW) system is using their data contained in other VA IT systems, this PIA does serve as notice of the system's existence and its PII collection, use, maintenance, and dissemination practices. This PIA is available online for public notification, review, and use, as required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii).

**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*

FCM does not directly collect the information displayed in the system. The information is pulled from other VA systems (FEE, FMS, HRPAS). Any opportunity to decline to provide would be handled through the originating system.

**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*

FCM does not directly collect the information displayed in the system. The information is pulled from other VA systems (FEE, FMS, HRPAS). Any opportunity to decline to provide would be handled through the originating system.

**6.4 PRIVACY IMPACT ASSESSMENT: Notice**
*Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.*

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

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

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

**Privacy Risk:** There is a risk that members of the public may not know that the Financial Content Management System exists within the Department of Veterans Affairs.

**Mitigation:** The VA mitigates this risk by providing the public with two forms of notice that the system exists, including the Privacy Act statement and a System of Record Notice.

## Section 7. Access, Redress, and Correction

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

**7.1 What are the procedures that allow individuals to gain access to their information?**

*Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. For example, if your program has a customer satisfaction*

*unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.*

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

*If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.*
*This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.*

FCM does not directly collect the information displayed in the system. The information is pulled from other VA systems (FEE, FMS, HRPAS). Any opportunity to review and correct would be handled through the originating system.

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

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

Under the jurisdiction of VHA, VHA Handbook 1605.1 "Right to Request Amendment of Health Information", the individuals must submit a written request which includes designated record sets, as provided in 38 CFR 1.579 and 45 CFR 164.526. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and be filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

**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.*

FCM does not directly collect the information displayed in the system. The information is pulled from other VA systems (FEE, FMS, HRPAS). Any opportunity to review and correct would be handled through the originating system.

**7.4 If no formal redress is provided, what alternatives are available to the individual?** *Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.*

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

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

There are no alternatives. FCM does not directly collect the information displayed in the system. The information is pulled from other VA systems (FEE, FMS, HRPAS). Any opportunity to review and correct would be handled through the originating system.

**7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction**

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

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

**Privacy Risk:** The risk of inaccurate data lies with the originating system, whereby individuals may provide incorrect information in the originating system and do not correct it. FCM does not directly collect the information displayed in the system. The information is pulled from other VA systems (FEE, FMS, HRPAS). Any opportunity to review and correct would be handled through the originating system.

**Mitigation:** Individuals provide information directly to the users of FEE, FMS, and/or HRPAS. Any validation performed would merely be the individual personally reviewing the information before they provide it. Individuals are allowed to provide updated information for their records by

submitting new forms or correspondence and indication to the VA that the new information supersedes the previous data.

## Section 8. Technical Access and Security

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

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

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

*Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?*

*Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.*

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

The FCM, FEE, FMS, and HRPAS staff and several Austin Information Technology Center staff who maintain the systems have national access to perform their duties. VACO staff and Stations have restricted access to FCM, FEE, FMS, and HRPAS data. Stations are limited to data for that station. Access is limited to the scope of responsibility required for each VA employee to perform their duties where it is at VACO or at a station. FCM users have access limited to the population of information they serve.

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

*If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII.*

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

Contractors can be granted access to FCM if their VA manager and local Information Security Officer approve. They are required to follow the same procedures VA employees do for access, which is to submit a 9957 form as specified in section 8.1. In addition, in accordance with the contract between the contractor and the government, all contractors with access to FCM information are required to meet the AITC contractor security requirements. Contracts are reviewed annually by the Contracting Officers Representative.

**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.*

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system.

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

*If Yes, provide:*

1. *The Security Plan Status,*
2. *The Security Plan Status Date,*
3. *The Authorization Status,*
4. *The Authorization Date,*
5. *The Authorization Termination Date,*
6. *The Risk Review Completion Date,*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

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

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

The Security Plan Status is Authority To Operate (ATO).

The Security Plan Status Date Is September 1st of 2022.

A full 3-year Authority to Operate (ATO) was granted on 01/11/2021 (1095 days), and expires 1/11/2024.

The risk assessment was completed September 1st of 2022.

This system is categorized as a high.

## Section 9 – Technology Usage

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

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

*If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS).*

*This question is related to privacy control UL-1, Information Sharing with Third Parties.*

*Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1.*

N/A

**9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract)**

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

N/A

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

*Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.*

*This question is related to privacy control DI-1, Data Quality.*

N/A

**9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?**

*What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met?*

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

N/A

**9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.**

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

N/A

## Section 10. References

Summary of Privacy Controls by Family

*Summary of Privacy Controls by Family*

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

| ID | Privacy Controls |
|---|---|
| UL-1 | Internal Use |
| UL-2 | Information Sharing with Third Parties |

**Signature of Responsible Officials**

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

Gina A Siefert 273290

Digitally signed by Gina A Siefert 273290
Date: 2022.11.15 07:30:37 -06'00'

**Privacy Officer, Gina Siefert**

Tamer F. Ahmed 531244

Digitally signed by Tamer F. Ahmed 531244
Date: 2022.11.15 13:05:54 -05'00'

**Information System Security Officer, Tamer Ahmed**

DAVID LARSON

Digitally signed by DAVID LARSON
Date: 2022.11.16 08:26:44 -06'00'

**Information System Owner, David Larson**

## 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).