‘

Privacy Impact Assessment for the VA IT System called:

Financial Reports Management (SNW)

Financial Business Operations

Systems Administration

Date PIA submitted for review:

02/08/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Tonya Facemire	tonya.facemire@va.gov	202-632-8423
Information System Security Officer (ISSO)	Neil Cruz	Neil.Cruz@va.gov	202-632-7422
Information System Owner	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 VA Financial Reports Management (SNW) uses SnapShot Technologies' SnapShot Web to provide VA customers with generated reports for Financial and Human Resources (HR) data. SnapShot Web is a commercial off the shelf product that provides a digital report management solution that centralizes report data access and provides controlled security to the data. Each VA field station controls and maintains its own security processes. However, the application and database reside within the Austin Information Technology Center (AITC).

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. The IT system name and the name of the program office that owns the IT system.

Financial Reports Management (SNW) is owned by the Financial Management (FM) program office.

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

Financial Reports Management (SNW) uses security controls, authorizing select VA employees, permitting enhanced capabilities for viewing the Financial Management System (FMS) generated reports.

SNW enables authorized VA employees online viewing of secure FMS reports with an intranet browser using the VA Intranet, instead of the mainframe.

The FMS report information is not verified or modified and is only displayed using the Financial Reports Management (SNW) product. FMS uses this information in SNW to integrate VA's accounting systems and reports financial services and information to all VA organizations.

C. Indicate the ownership or control of the IT system or project.

Ownership control is given to the business owner, Director of FMS Albert Smalls.

2. Information Collection and Sharing

D. The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.

There are approximately 1.5 million vendors in the system. However, no information on individual people is kept in the system, only invoices to companies. These are companies supplying goods or services to the VA.

E. A general description of the information in the IT system and the purpose for collecting this information.

Financial Reports Management consists of a database for storing reports and a Web application that allows authenticated users to retrieve reports from the database through a browser accessing the VA Intranet. Here are some of the report titles:

- Medical Care Appropriations
- Detail Accounting Transactions
- Obligations By Budget Object Code
- Unfunded Expense Report
- Reconciliation Of General Ledger Accounts

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

The reports are created by FMS and are available for viewing on the mainframe, but for research purposes, enhanced viewing capabilities are nonexistent. Most recently, CDs containing these reports were generated by the VA and delivered to FMS customers, but this led to security concerns.

G. 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.

The VA Financial Reports Management system displays Personally Identifiable Information (PII) from Veterans, other members of the public, and VA employees and contractors. The information depends, in part, on the types of reports being created. The server is located on the internal VA network only and is not accessible by the public. Authorized personnel can be defined as those who have passed background checks, completed security training, agreed to the VA Rules of Behavior, and have submitted the appropriate access request to the proper channels. The reports are needed to allow them to ensure vendors are paid correctly, process claims, and correctly process veteran benefits.

3. Legal Authority and SORN

H. A citation of the legal authority to operate the IT system.

The following laws and regulations affect Financial Reports Management:

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

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?

A SORN does not need to be made for FRM, as it is not a system of record. It also not a cloud service.

D. System Changes

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

No.

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

No.

Section 1. Characterization of the Information

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

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

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

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

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

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

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

PII Mapping of Components (Servers/Database)

Financial Reports Management (SNW) consists of one key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by (SNW) 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 the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Database Connections

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	No	N/A	N/A	VA, ITOPS Datacenter and application staff have implemented required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA Handbook 6500, Risk Management Framework for VA Information Systems.

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?

N/A

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.

N/A

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

The FMS mainframe application provides the information to Financial Reports Management (SNW). SNW does not collect data directly from any internal or external entities. The system displays only the pre-generated reports that FMS provides.

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?

All information is received via electronic transmission. Financial Reports Management (SNW) utilities convert the reports to PDF format and store them on the server.

1.3b 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.

The FMS mainframe application provides the information to Financial Reports Management (SNW). SNW does not collect data directly from any internal or external entities. The system displays only the pre-generated reports that FMS provides. It does not collect paper forms.

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.

1.4b 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.

The information used by Financial Reports Management (SNW) is collected from the FMS system. Financial Reports Management (SNW) assumes the accuracy of the information collected from the FMS system and does not do any additional accuracy verification. Authorized personnel for FMS review the reports for accuracy. For more information on the FMS system, please go to VACO Privacy website for all VA PIAs at https://www.oprm.va.gov/privacy/pia.aspx

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

All Austin Information Technology Center (AITC) information systems, including Financial Reports Management (SNW), enforce assigned authorizations for controlling access to the system in accordance with applicable policy.

All systems that store, process, or transmit sensitive information use a properly maintained and configured version of an authentication-based access control system to ensure that the sensitive information is not improperly disclosed, modified, deleted, or rendered unavailable. A list of all users who have access (even read-only) to certain types of data is reviewed quarterly.

The following laws and regulations affect the SNW system:

- Federal Managers Financial Integrity Act of 1982 (FMFIA)
- OMB Circular A-123 - "Internal Control Systems"
- OMB Circular A-130 - "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Resources"
- Federal Information Security Management Act of 2002 (FISMA) (Title III, 2002 E-Gov Act)
- OMB M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
- Executive Order 13103, "Computer Software Piracy"
- Government Paperwork Elimination Act (GPEA), PL 105-277
- Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191
- Information Technology Management Reform Act of 1996 (also known Clinger-Cohen Act of 1996 (40 United States Code 1452))
- 5 U.S.C. 552a, "Privacy Act of 1974," 5 United States Code 552a, Public Law 99-08, c. 1974.

- 5 U.S.C. 552, “Freedom of Information Act,” 5 United States Code 552, c. 1967
- 18 U.S.C. 1030 (a) (3), "Fraud and related activity in connection with computers."
- 18 U.S.C. 1001, Computer Fraud and Abuse Act of 1986.
- Electronic Communications Privacy Act of 1986, Public Law 99-08, 100 Stat. 1848
- 17 U.S.C. 106, “Exclusive rights in copyrighted works”
- 38 U.S.C. 218, "Security and law enforcement on property under the jurisdiction of the Veterans Administration"
- 38 U.S.C. 3301, "Confidential nature of claims"
- Federal Information Processing Standards (FIPS)
    - FIPS 199, “Standards for Security Categorization of Federal Information and Information o Systems”
    - FIPS 200, “Minimum Security Requirements for Federal Information and Information Systems”
    - FIPS 201, “Personal Identity Verification of Federal Employees and Contractors”
    - FIPS 140-2, “Security Requirements for Cryptographic Modules”

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:

Data maintained in the Financial Reports Management (SNW) database is classified as a mixture of Sensitive and Non- Sensitive. For example, financial information and PII is obtained from the Financial Management System (FMS) application. The breach or accidental release of information to inappropriate parties or the public could result in financial, personal, and/or emotional harm to the individuals whose information is contained in the system.

Mitigation:

- Financial Reports Management (SNW) data is protected from unauthorized modification (data is not editable).
- Access is through the VA network via secure web interface; there is no public facing interface.
- The system adheres to information 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.

SNW collects and maintains pre-generated reports from FMS, not individual pieces of information.

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

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.

N/A

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.

SNW simply acts as a viewer of FMS reports created on the mainframe.

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?

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

Data at rest is encrypted and as the data is transmitted it is done with a secure connection as well.

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

AITC Directive/Handbook 0710 Personnel Security, Part 5 - Security and Privacy Awareness Training requires all personnel with root- or administrator-level access to information systems, including SNW, to receive adequate training within 30 days of appointment to their position.

Security training is required annually for all AITC employees and VA customers who maintain or use SNW. Office of Cyber and Information Security (OCIS) keeps records of all completed security training.

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?

The PIA is clear on the use of the information contained in the system relevant to the mission of the project. SNW is used in support of the AITC mission, which is to provide cost-efficient IT enterprise solutions to support the information technology needs of customers within the Federal sector. Customers can view reports quicker than they can view the mainframe reports, and the search features in SNW are very helpful for analyzing the data.

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?

A VA form 9957 is submitted to the FRM requests VA email account, and a SNW ticket is created. The group becomes aware of the request through this request, and a system administrator is assigned to review the request. The administrator can decide based on details on the form.

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?

The VA manages security and monitors for any breaches.

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

Financial Reports Management (SNW) processes all the VA data to PDF frames viewable by the SNW software in report format. The information retained in the report is dependent on the report on which the information is displayed.

The system retains only the pre-generated reports that FMS provides. These retained reports may contain name, SSN, DOB, personal mailing address, personal phone number, financial account information and race/ethnicity.

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.*

FMS reports are retained online for all active VA employees via reporting tools. The data is archived on tape, transferred to a records facility for three or more years.

NARA's General Records Schedule (GRS), Transmittal 29, is a GRS for Financial Management and Reporting Records (GRS 1.1), stating longer retention is authorized if required for business use; therefore, the data retention schedule is dependent upon FMS.

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

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

Yes.

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

FMS reports are retained within the rules of the General Records Schedule (GRS), ERA Number DAA-GRS2013-0005 GRS 3.1-General Technology Management Records (archives.gov). Records contained in the VA FMS system will be retained as long as the information is needed in accordance with a NARA approved retention period.

3.4 What are the procedures for the elimination 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.

Currently, SNW reports are retained indefinitely. FMS has its own retention schedule and SNW receives reports from them. NARA's General Records Schedule (GRS), Transmittal 29, is a GRS for

Financial Management and Reporting Records (GRS 1.1), stating longer retention is authorized if required for business use.

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

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

Yes. The system minimizes the risk to privacy of using PII for testing by masking PII in test reports. New reports are first created and set up under a special station that is accessible only to users who will be testing. There is no test server. Test reports reside on the production server during testing and are removed once testing is complete.

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:

Since the reports stay in the system indefinitely, the impact of a security breach is greater. Unauthorized access would be to all Financial Reports Management (SNW) reports created since 2005.

Mitigation:

SNW has security and access controls in place to reduce the risk of unauthorized access. Audit logs record event type, date and time of event, user identification, workstation identification, success or failure of access attempts, and security actions taken by system administrators or security officers. If an approved user does not access Financial Reports Management (SNW) in 90 days, their access is removed. SNW resides within the LAN and is included in the AITC Accreditation Boundary that has an Authority to Operate (ATO). No one can access the reports without being authorized through the VA security procedures.

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***
N/A/	N/A	N/A	N/A

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: Privacy information may be release to unauthorized individuals.

Mitigation:
All personnel with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually. The knowledge gained from this reduces the chances of them releasing unauthorized information.

Audit logs record event type, date and time of event, user identification, workstation identification, success or failure of access attempts, and security actions taken by system administrators or security officers. If an approved user does not access Financial Reports Management (SNW) in 90 days, their access is removed. Financial Reports Management (SNW) resides within the LAN and is included in the AITC Accreditation Boundary that has an Authority to Operate (ATO). No one can access the reports without being authorized through the VA security procedures.

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***	***List the method of transmission and the measures in place to secure data***

			more than one)	

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

Follow the format below:

Privacy Risk:
Privacy information may be released to unauthorized individuals.

Mitigation:
The Financial Reports Management (SNW) system does not share Personally Identifiable Information (PII), Sensitive Personal Information (SPI), or Protected Health Information (PHI) with any external organizations, IT systems, or government agencies. All personnel with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually. The knowledge gained from this reduces the chances of them releasing unauthorized information.

Section 6. Notice

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

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy

policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

The Financial Reports Management (SNW) system displays information from VA application FMS, instead of directly from Veterans, members of the public, or other individuals. As such, the system does not provide individuals with direct notice that it is collecting and using their information. It is assumed that these applications do provide direct notice to individuals prior to collecting information from them.

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

It is assumed that the serving applications provide notice to individuals prior to collecting information from them. FRM is not a system of record and does not store this information, and so does not provide notice accordingly.

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.

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.

Individuals' ability to decline to provide information is based on the needs and practices of the originating VA IT systems: FMS. Please review the PIAs and applicable SORN for this system to learn more. Individuals do not have the opportunity to decline to provide information to Financial Reports Management (SNW) because information is not collected directly from them.

The VA authority to collect PII is documented in the System of Records Notice (SORN) and Privacy Act Statement.

Privacy Impact Assessments (PIA) are available at: https://www.oprm.va.gov/privacy/pia.aspx

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.

Individuals may have the right to consent to uses of their information as collected and used by the originating VA IT systems. Please review the applicable PIAs and SORNs to learn more. However, individuals are not given the opportunity to consent to their information being used by Financial Reports Management (SNW), as the system is used to create and view important reports used by the VA to carry out its mandated duties.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (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 application FMS will not know how their information is being shared and used internal to the Department of Veterans Affairs and will be unaware that the VA is using Financial Reports Management (SNW) to create reports about VA financial issues.

Mitigation:

This PIA serves to notify individuals of the Financial Reports Management (SNW) system and includes information about the collection of information from these systems (see questions 1.2, 1.3, and all of Section 6.

The SNW system does not have a SORN, as it is not a system of record.

Section 7. Access, Redress, and Correction

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

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

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

The Financial Reports Management (SNW) system does not have procedures in place to allow individuals to gain access to their information in the system. As the system is not a System of Record (a system which pulls information using a unique identifier such as name or SSN) it is not possible to produce a record for an individual to review. Any changes to the Financial Reports Management (SNW) Veteran information are made through the FMS application and transferred to Financial Reports Management (SNW). Personal information held in the originating VA application FMS – may be accessible to individuals. Please review the applicable PIA and SORN for more information. The SNW system does not have a SORN of its own, as it is not a system of record.

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).

The data in the system is not retrieved by a personal identifier, and therefore is not subject to the access provisions of the Privacy Act.

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.

An individual does not have access to information in the FRM system. The data in the system is not retrieved by a personal identifier, and therefore is not subject to the access provisions of the Privacy Act.

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.

The Financial Reports Management (SNW) system does not have procedures in place to allow individuals to correct inaccurate or erroneous information in the system. As the system is not a System of Record (a system which pulls information using a unique identifier such as name or SSN) it is not the origin of the information. Any changes to the Financial Reports Management (SNW) Veteran information are made through the FMS application and transferred to Financial Reports Management (SNW). Personal information held in the originating VA application FMS and may be accessible to individuals. Please review the applicable PIA and SORN for more information.

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.

The Financial Reports Management (SNW) system does not have procedures in place to allow individuals to correct their information in the system. As the system is not a System of Record (a system which pulls information using a unique identifier such as name or SSN) it is not possible to produce a record for an individual to review. Personal information held in the originating VA application FMS may be accessible to individuals for correction or redress. Please review the applicable PIA and SORN for more information.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

The Financial Reports Management (SNW) system does not have procedures in place to allow individuals to correct their information in the system. As the system is not a System of Record (a system which pulls information using a unique identifier such as name or SSN) concerned

individuals must contact the originating VA application FMS – who may have procedures for correction or redress. Please review the applicable PIA and SORN for more information.

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 in Financial Reports Management (SNW), there is a risk that the system may use inaccurate data when creating reports.

Mitigation:
Overall security for Financial Reports Management (SNW) is provided by AITC personnel and procedures. These procedures include providing change control for the server connectivity, providing physical security for the equipment, and providing security for access to the information system. AITC system administrators keep the Financial Reports Management (SNW) server up to date with all latest software security patches and new software applications where indicated. Accounts are disabled after 180+ days of dormancy or inactivity. There is no logon or password for authentication to Financial Reports Management (SNW). Access is granted from their PIV badge ID once logged into the network. The above measures help to ensure that information is safeguarded to maintain confidentiality, integrity and availability. Additionally, fiscal/budget analysts and other analysts in the field review reports as they are generated, and immediately bring anomalies to the attention of the respective system's staff.

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.

Per VA Directive and Handbook 6330, every 5 years the Office of Information Technology (OIT) develops, disseminates, and reviews/updates a formal, documented policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; along with formal, documented procedures to facilitate the implementation of the control policy and associated controls. Here are the specific procedures to get access to Financial Reports Management (SNW): Fill out VA Form 9957 electronically (not manually) and use the appropriate Functional Task Code (FTC): 104SW01, for FMS.

Do NOT include your Social Security Number!

Include the following information:
User's LAN ID
User's Name and Phone Number
User's Station Number
Concurring System Manager of Record (Approving Official)
Requesting Official (cannot be the same as approving official and vice versa)
Approving Official's digital signature – MUST be a valid digital signature (no unknown or invalid)
Active Directory (AD) Username
Active Directory (AD) Domain
Email Address Version
ISO digital signature is now optional and decided by each individual station

Have the Concurring System Manager of Record submit the 9957 through a digitally signed email to your designated IAMS POC. The Concurring System Manager of Record is usually the applicant's supervisor. Public Key Infrastructure (PKI) digital certification of the email is required while encryption is unnecessary. Please do not encrypt the email before submitting to the IAMS POC. Do NOT encrypt when submitting request to snapwebrequests@va.gov. Do not use 9957 forms dated prior to October 2016. E9957s are acceptable as long as they are completed correctly. A new required field, AD username has been added to determine exactly which user in case of identical first and sir names.

The POC or ISO will forward the email and the attached 9957 request from the Concurring System Manager of Record to SNAPWEB REQUESTS. The forwarded email will provide an audit trail of the 9957 request. Not even, in some cases, does the approving official have the final approval of the

access requested. Final determination may be determined by the FRM group, as we only grant the access necessary.

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?

No other government agencies have access to the FRM system.

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.

All customers only have read access. They cannot edit data in FRM.

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 Financial Reports Management (SNW) if their VA manager and ISO approve. They are required to follow the same procedures VA employees do for access, which is to submit a 9957 form as specified in section 8.1.

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

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

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

training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Completed
2. *The System Security Plan Status Date:* March 3, 2022
3. *The Authorization Status:* ATO
4. *The Authorization Date:* March 22, 2022
5. *The Authorization Termination Date:* March 22, 2023
6. *The Risk Review Completion Date:* Jan. 24, 2023
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.***

Authorization and Accreditation (A&A) has been completed. SNW is a Medium System with an active full Authority to Operate (ATO) granted on 03/22/2022 and expires on 03/22/2023.

Section 9 – Technology Usage

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

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

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

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

Financial Reports Management (SNW) does not use cloud technology.

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.

Financial Reports Management (SNW) does not use cloud technology.

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.

Financial Reports Management (SNW) does not use cloud technology.

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.

Financial Reports Management (SNW) does not use cloud technology.

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).

Financial Reports Management (SNW) does not employ use of AI or Bots.

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**

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

Signature of Responsible Officials

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

Tonya L. Facemire 234776

Digitally signed by Tonya L. Facemire 234776
Date: 2023.03.09 14:12:13 -05'00'

Privacy Officer, Tonya Facemire

Neil F. Cruz 341838

Digitally signed by Neil F. Cruz 341838
Date: 2023.03.09 14:49:52 -05'00'

Information System Security Officer, Neil Cruz

DAVID LARSON

Digitally signed by DAVID LARSON
Date: 2023.03.09 13:59:47 -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).

HELPFUL LINKS:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

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

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

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