Privacy Impact Assessment for the VA IT System called:

Vendor Resource Management System (VRMS)

Veterans Benefits Administration

Date PIA submitted for review:

7/28/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Chiquita Dixson	Chiquita.dixson@va.gov	202-632-8923
Information System Security Officer (ISSO)	Anita Feiertag	Anita.Feiertag@va.gov	513-289-8116
Information System Owner	Berletney House	Berletney.House@va.gov	202-632-8812

Abstract

Vendor Resource Management System (VRMS) is the system that Vendor Resource Management (VRM) uses to manage the VA-acquired property inventory. Each Real Estate Owned (REO) property is assigned to VRM through a web service defined as New Property (NP) and is confirmed through a return Master Confirmation message (MC) web service. Once a property is confirmed to be in VRM, the entirety of the tasking performed by the contractor to manage an REO property for the VA is housed in the VRM system as a managed service. These processes include eviction, property preservations, repair, tax/HOA, title, pre-marketing, valuation, marketing, offer management, contracts, closing, and invoicing of the properties. These transmissions also transmit data back to VA for oversight purposes at specific intervals and the processing of post-disposition invoices related to the contract.

The application is internet based and includes external interfaces with VA Loan Guaranty Service (LGY) systems, available for all VA Loan Guaranty employees to access. VRM also provides access to operational reporting within their system and conducts reconciliation with our WebLGY system through a reconciliation web service.

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.

Vendor Resource Management System (VRMS) is the name of the IT System. This IT system has been developed, maintained, and operated by VRM Mortgage Services to facilitate the Department of Veterans Affairs (VA) Loan Guaranty Service (LGY) home loan program.

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

VRMS provides computing services in the form of servers offering Identification and authentication, email services, boundary protection devices and some web services. These services provide the IT and Communications infrastructure for the entire BAC.

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

The IT system is owned and operated by Vendor Resource Management.

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.

The VRMS system stores information about the following types of individuals: former owners, property occupants, and potential/actual purchasers. Former owners are the borrowers associated with the default loan that resulted in the REO. VRMS currently stores approximately 140,000 of these records, which consist of first and last names. Property occupants are individuals who occupy a property at the start of the REO process. VRMS currently stores approximately 270,000 of these records, including first name, last name, and phone number. About 60,000 of these records also include SSNs. Potential/actual buyers are individuals who submitted an offer to purchase an REO property. VRMS currently stores approximately 1,700,000 of these records, including first name, last name, phone number, email address, and address.

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

VRMS captures and stores information related to securing, marketing, and disposing REO of properties. This includes the following information: defaulted loan information, property information, property condition information, property repair information, tax information, HOA information, marketing information, offer information, and contract/closing information.

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

VRMS is integrated with WebLGY and uses this integration to exchange data with the VA. In addition, VRM vendors will access data through the VRMS web portal in order to complete REO-related tasks and activities.

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.

VRMS is deployed at two sites: Sungard Scottsdale, AZ (production) and Sungard Richardson, TX (DR). Both sites implemented the same security controls.

3. Legal Authority and SORN

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

U.S.C. § 5106 (Department of Veterans Affairs (DVA statute) requires the head of any Federal department or agency, including SSA, to provide information, including SSNs, to the DVA for purposes of determining eligibility for or amount of VA benefits, or verifying other information with respect thereto. SSNs are used extensively through the LGY Web Applications. End user SSNs are used to uniquely identify registered users of the Loan Guaranty (LGY) Veterans Information Portal (VIP). Veteran SSNs are used to validate eligibility requirements and rating information from the external systems.

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?*

No. See applicable SORNs below.

SORN: Loan Guaranty Home, Condominium and Manufactured Home Loan Applicants Records, Specially Adapted Housing Applicant Records and Vendee Loan Applicant Records-VA 55VA26: 79 FR 3922, 1/23/2014.

D. System Changes

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

No. There have been no business process changes since the last PIA was approved.

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

No. There have been no technology changes since the last PIA was approved

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.

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)

New Properties, Deactivation (DEACT), Real Estate Owned, Portfolio Loan Servicing Profile and Data, Withdrawal Decision, Fee, Invoice Status Processing (IPS), Property and Loan Origination, Loan History, Transaction and Boarding confirmations associated with a loan that is being actively serviced by VRM, New Property Confirmation (MC), HOA, Offer, Listing, Habitability, INV (AI, SI, VI, MI, Tax/Scrub), Daily Remittance, Partial Claim Loans Identification Number. A full list of data elements for the interface can be located by contacting the Contracting Officer Representative (COR) for this Managed Service or found in the following document available from the System Owner identified on Page 1 above: WebLGY- REO and Portfolio Servicing Contract (RPSC) Web Service Requirements Specification.

PII Mapping of Components (Servers/Database)

Vendor Resource Management System (VRMS) consists of **One** key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **VRMS** 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.

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
LGYPRD1	Yes	Yes	SSN/TIN, address, phone number; DOB, e-mail, race/ethnicity	Facilitate REO sales	HTTPS, SSL,TLS1.2, FIPS 140-3.

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

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

Information used in the performance of this contract comes from various VA-approved loan-servicing companies who service VA Guaranteed home loans, and who initiate their services when a home goes foreclosure. The Servicer will convey that property to WebLGY via the VA Loan Electronic Reporting Interface (VALERI) that sends information to VA, who then routes it to VRM via web services. WebLGY sends VRM information regarding the property and the former owner. VRM sends to WebLGY title/reconveyance information, property listing information, property offer information, origination number request, third-party withdrawal service request, HOA information as well as invoice information approval and reimbursement. BSI subcontractor of Vendor Resource Management Inc, will manage the servicing of VA owned loans.

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 that this is where the information is coming from and then indicate why the system is using this source of data.

VRM obtains information from only the VA or the individual.

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

VRMS contains reporting that is used by VRM to manage the REO process. This reporting is not used by 3rd parties.

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?

Information is collected from information systems as a result of business operations or changes to records disposition in the management of REO properties.

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.

Information is collected from information systems as a result of business operations or changes to records disposition in the management of REO properties.

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.

Loan Guaranty Service provides Contract Assurance oversight functions to ensure oversight and accuracy of information. In addition to these functions, VRM participates in a yearly Statement on Standards for Attestation Engagements (SSAE) 18 Service Organization Control (SOC) 1 assurance services review as conducted by Grant Thornton.

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.

VRM does not obtain information from commercial aggregators.

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 authority for this Agreement is based on Task Order: VA119A-17-C-0062 issued by the VBA of Department of Veteran Affairs on 6/1/2017. The intent of this agreement is to provide VBA with an efficient, accurate, and secure data transmission of Loan data that deals with maintenance, sale, and servicing of VA acquired properties. This Agreement protects all Veteran information during processing, storage, and transmission to and from VBA. VBA has authority to disclose information being provided to VRM and USDA under Title 5, USC, Section 552a, Privacy Act of 1974, and routine use 60 of the System of Records entitled "Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA" (58VA21/22/28), published at 74 FR 29275, June 19, 2009, last amended at 77 FR 42593, July 19, 2012 and:

- Privacy Act of 1974, 5 U.S.C. § 552a;
- VA Directive and Handbook 6500, Information Security Program.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?
This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk: Given the nature and sensitivity of the information as indicated in Sec. 1.1, the breach of such information could result in damage to the information owner, such as identity theft or related fraud.

Mitigation: To mitigate the risk, access to SPI/PII data maintained by VRM is limited to only those individuals needing and authorized to have such access to perform the tasks contracted for by VA. In addition, SSN detail is encrypted at rest, and use of such information is logged and reviewed as needed to ensure accesses are authorized and appropriate.

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.

1. **Name:** Used to identify borrowers
2. **Social Security Number**: Used as a unique identifier for borrowers.
3. **Date of Birth**: Used for identity verification and to ensure accuracy of borrower records.
4. **Race/Ethnicity:** Used to provide socio-economic reporting on vendor network and spend.
5. **Personal Mailing Address**: Used to send communications and documents related to loans.
6. **Personal Phone**: Used as a contact method for communications or loan-related matters
7. **Personal Email:** Used as a contact method for communications or loan-related matters
8. **Tax Identification Number**: Used to identify third-party vendors and to fulfill tax reporting requirements.
9. **Other Data Element:** The above mentioned data elements are used to process federally backed mortgage loans for its government business partners and are included in the following transactions: Loan Boarding, Electronic File Delivery, Data Mapping, Data Conversion, Acquisitioning Processes, Exception Processes and Approvals, Default Management, Portfolio Communications, Master Servicing, Fees Due, Property Management, Master File (Corrections & Audit), Remittance Processing, Customer Service, Tax Services & Management.

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.

Veteran and asset data provided to VRM by VA are utilized as-is. No complex analysis of such data is needed, and no additional records are developed using that data.

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.

NA

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?

VRM has implemented numerous physical, administrative and logical policies and procedures to ensure the continued confidentiality of all PII/SPI entrusted to VRM. Change management policies and procedures govern alterations and testing of software. SPI is encrypted at rest where appropriate, and over secure links when in transit. Computers which may contain PII/SPI employ full disk encryption. Two-factor authentication is utilized when connecting to corporate Internal data and systems remotely. System access will time-out after appropriate periods of inactivity. PII/SPI data is always used and stored in secure environments. Audits and reviews are performed regularly to ensure controls are operating effectively. Incident response plans are in place and tested to identify and effectively respond to potential security incidents.

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

SPI is encrypted at rest where appropriate and over secure links when in transit. Computers which may contain PII/SPI employ full disk encryption. Two-factor authentication is utilized when connecting to corporate Internal data and systems remotely. System access will time-out after appropriate periods of inactivity. PII/SPI data is always used and stored in secure environments. Audits and reviews are performed regularly to ensure controls are operating effectively. Incident response plans are in place and tested to identify and effectively respond to potential security incidents

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

VRMS meets or exceeds Privacy and Audit Controls as identified in the eMASS record.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. ***Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.***

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

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

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?

This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

2.4a How is access to the PII determined?

Veteran and asset data provided to VRM by VA is utilized in accordance with SORN 55VA26, 17VA26 and 58VA21/22/28, as well as in accordance with VA/VRM contract terms, and is never shared with unauthorized personnel. All data considered to be SPI/PII is protected from unauthorized access, and is encrypted wherever deemed necessary. All VRM personnel with access to veteran's data are required to take "VA Privacy and Information Security Awareness and Rules of Behavior" training annually, such training is tracked and enforced, and access to VA data is removed for anyone failing to take such recurring training timely. Additionally, all VRM personnel are required to take VRM's internal IT Policy & Privacy training annually, and such training is tracked and enforced.

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

Yes. VRM has implemented controls to limit access to PII to only individuals that have a business need to access the data.

2.4c Does access require manager approval?

Manager approval is required for a user to be assigned a security role that would grant access to PII.

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

Yes. Access and modification to PII is tracked and recorded. VRM reviews these logs for anomalous activity

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

VRM's ISO is responsible for assuring safeguards for PII within VRM's IT systems.

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

Veteran name, SSN, mailing addresses with ZIP codes, email address, and phone numbers (as identified in Section 1.1) are the items of information retained in the VRM system.

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.*

Per specific terms provided in the contract between VRM and VA, SPI/PII and non-SPI/PII data are transferred to and retained at the VA for three years after the contract with VRM Mortgage Services ends. Such data will then be destroyed from VRM's records only after receiving written approval from VA's Compliance Officer. (See section 3.4 for post-contract destruction detail.)

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

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

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

The records retention schedule is described in Veterans Benefits Administration Records Control Schedule VB-1, Part I, Field. See Section XII for retention schedule of individual items of record. There are different requirements for different parts of this program, but the data at the end goes into the original loan file that is sent to the federal records center after the last action taken (sold, claims paid, etc.) with one exception on mobile homes documents are destroyed 32 years after retirement. (Retirement means close out of last action on these records and sent to FRC). This information is located at http://www.benefits.va.gov/WARMS/docs/admin20/rcs/part1/VB-1Part-I.doc.

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

VB-1, Part 1, Section XIII, Item 13-052.100

http://www.benefits.va.gov/WARMS/docs/admin20/rcs/part1/VB-1Part-I.doc

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.

Data provided by the Veterans Administration is retained by VRM for the period described in Section 3.2 above, and is purged from VRM records only after receiving written permission from the Contracting Officer CO. Thereafter, data retained by VRM can be purged from active VRM databases, after being provided to VA in accordance with SORN 55VA26, Records in individualized case folder concerning active VA guaranteed or insured loans are retained at the VA servicing facility for up to three years and forwarded to the Federal Archives and Records Center (FARC). Any subsequent retention of such data will be managed by the Federal Archives and Records Center (FARC) as identified in Section 3.3 above. As per CO approval, data will be backed up to disk within VRM at Sungard Data Services (in accordance with VRM's managed backup services contract) will be removed from active databases within 30 days, or earlier if requested by VA. Tape backups, which are taken monthly and retained indefinitely, will be purged, destroyed, degaussed or overwritten upon subsequent written request by VRM to Sungard to eliminate such data. Additional VRM procedures for eliminating data are documented in the SSP, and in the Sungard Managed Backup Services agreement. All specific procedures performed by Sungard in the elimination process are documented by Sungard.

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.

VRM does not utilize PII in any form of testing. Even during QA testing, any PII or confidential data is dummied-out in the process of creating the QA environment.

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: Extended and/or unnecessary retention of SPI/PII data such as SSN's and mailing addresses increases the likelihood of a potential breach of such information.

Mitigation: Mitigation is best achieved by ensuring that sensitive data is removed/archived/destroyed as soon as is feasible under the terms of the associated SORNs, contracts and agreements.

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?

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.

Veterans Benefits Administration (VBA), system Loan Guaranty (LGY) exchanges include new properties (NP), Deactivation (DEACT), Reconveyance Decision, Withdrawal Decision, Fee, Invoice Status Processing (IPS) information, and VA user status requests. This interconnection is a two-way

data exchange path between VA and VRM. This interconnection is encrypted through compliant Web Service (HTTPS).

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Veterans Benefits Administration (VBA)	Purpose of validating and transferring the subordinate mortgage into servicing.	Data to be exchanged includes new properties (NP), Deactivation (DEACT), Reconveyance Decision, Withdrawal Decision, Fee, Invoice Status Processing (IPS) information, and VA user status requests.	This interconnection is a two-way data exchange path between VA and VRM. This interconnection is encrypted through compliant Web Service

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: Exposure of information to personnel within VRM and with our loan servicing partners increases the likelihood that such data may be breached or shared inappropriately, resulting in substantial harm, embarrassment, and inconvenience to individuals and may lead to identity theft or other fraudulent use of the information.

Mitigation: Privileges to access any VRM systems and data containing VA-related information, especially any SPI/PII, are only granted based on the user's role within VRM, and only to those with a need-to-know. Such privileges are authorized by Human Resources, or as directed by authorized senior management in accordance with VRM internal policies and controls. Access privileges for all users are reviewed and verified at least quarterly, and privileges for terminated users are removed within 24 business hours upon termination. Users without a need to modify asset related information are provided with "read-only" privileges and cannot make changes. Information-sharing agreements have also been implemented between VRM and BSI Financial, which outlines the acceptable mechanisms for exchanging data.

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.

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***
BSI Financial, Servis One, Inc. dba BSI Financial Services	To manage portfolio loan servicing for VA NADL, refunded/ repurchased and vendee loans.	Borrower name, property and loan origination, loan history, transaction and boarding confirmations associated with a loan that is being actively serviced by VRM. Full name, Social Security Number, date of birth, race/ethnicity, taxpayer identification number, and address (mailing and email)	ISA/MOU; SORN: Loan Guaranty Home, Condominium and Manufactured Home Loan Applicants Records, Specially Adapted Housing Applicant Records and Vendee Loan Applicant Records-VA 55VA26: 79 FR 3922, 1/23/2014	SFTP
VRMS, Vendor Resource Management (VRM)VRM	The interconnection between VRM and Loan Guaranty Service (LGY) is for the express purpose of exchanging loan guaranty information that will facilitate the accuracy of the guaranty	Borrower name, property and loan origination, loan history, transaction and boarding confirmations associated with a loan that is being actively serviced by VRM. Full name, Social Security Number, date of birth, race/ethnicity, taxpayer identification number, and address (mailing and email)	ISA/MOU	Web Services; SFTP

	information maintained by VA and VRM.			
Partial Claims, Vendor Resource Management (VRM)	Web service exchange between VRM/VA to receive boarding of a partial claim for servicing loading, process quality assurance and send confirmations of servicing boarding.	Data to be exchanged includes web services to board, review and service Partial Claim loans.	pending	Web Services

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: The overall risk is that veterans' SPI/PII may be used or shared inappropriately by VRM if contractual requirements and commitments are not complied with, potentially resulting in substantial harm, embarrassment, and inconvenience to individuals and may lead to identity theft or other fraudulent use of the information.

Mitigation: For work performed by VRM and any VA data provided to VRM for that purpose, an ISA and MOU are in place governing the transmission and use of all such data. VRM is audited yearly or near-yearly by OIG as needed to ensure compliance with the ISA/MOU. Also, see Sections 1.6 and 2.3 above for additional mitigation in place.

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.

In reference to this section, all authoritative data is obtained and managed by VA, then provided to VRM. VRM relies on VA to address the issues identified within this section. VRM does not interface directly with veterans in any manner that might identify inaccuracies of veteran information. VA provides veterans with options for identifying erroneous personal information, and a means to correct that information in VA records. Demographical information is collected through the vendee loan program on the Demographic Information Addendum. Borrowers can decline to provide this information without any denial of services. Additional disclosures on borrower's rights to financial data collections are authorized by borrowers through the Borrower's Certification and Authorization document within the Vendee Loan Program and executed versions are captured within the data record within originations and transferred to servicing as a part of the permanent record. Uniform Residential Loan Application and its data (URLA, 1003) authorize the lender to use such information as directly provided by the borrower for the processing, evaluation and management of the loan. Other mortgage collateral documents required through the loan origination program (W9, Federal Loan Collection, Note, etc. each have an authorization and/or penalty informing the borrower of their rights).

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

Please provide response here

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.

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.

Within the loan origination program, there are several areas in which a borrower can provide optional information without a denial of service (e.g., demographical information). There are some areas where if the information is not provided by the borrower, then a service (e.g. loan origination) cannot be given. Borrowers are informed through various documents (e.g. URLA) that failure to provide accurate information could impact the ability for the VA to process a loan.

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.

In providing the information, the borrower authorizes the right to use through an execution of their residential loan application and subsequent mortgage documents and disclosures.

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:
Privacy information provided by borrowers is used only for the purpose of facilitating a loan or servicing the loan. This information is limited to only those groups with the responsibility to provide originations, servicing or auditing of those service divisions.

Mitigation:
N/A – no mitigation required by VRM.

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.***

All authoritative data is obtained and managed by VA, then provided to VRM. VRM relies on VA to address the issues identified. Veterans have to contact VA Local Office to identify erroneous personal information and determine a means to correct that information in VA records. In the case of vendee loans, VRM does interact with veterans for securing a vendee loan.

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

N/A

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

N/A

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.

VRM allows for post-consummation in origination and servicing when we need to correct veteran information for portfolio loans.

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.

For loan-related information, veterans get regular statements from the loan servicers showing what their information is, and who to call if corrections are needed. VRM does interact with veterans for securing a vendee loan. Veterans have to contact VA Local Office to identify erroneous personal information and determine a means to correct that information in VA records.

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.

In addition to 7.3 above, borrowers have access to their information in both originations and servicing through secure borrower portals, separate from VRM.

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:
This risk is not applicable to the services contracted of VRM by VA. See Section 7.1 above for additional clarification.

Mitigation:
N/A – no mitigation required by VRM.

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.

Privileges to access any VRM systems and data containing VA-related information, especially any SPI/PII, are only granted based on the user's role within VRM, as well as Servicing and Originations personnel, and must have a "need-to-know". Such privileges are authorized by Human Resources, or as directed by authorized senior management in accordance with VRM internal policies and controls. Privileges for terminated users are removed within 24 business hours of notification, and privileges for all such users are reviewed and verified at least quarterly. Users without a need to modify asset related information are provided with "read-only" privileges and cannot make changes.

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 agencies have access to VA data in VRMS.

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.

VRMS uses a role-based security system to grant users access to view/edit data. Users are assigned the role with the least permissions that allows them to perform their job duties.

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.

The VRMS application is developed, maintained, and hosted by Vendor Resource Management (VRM), who is a VA contractor. VRM uses role-based security to limit access to VA information, including PII, to those individuals that need access based on job function. VRMS logs all requests to view PII and these logs are regularly monitored by VRM to ensure that all access requests are justified.
In addition, VRM grants access to information using the principle of least privilege and minimizes the number of individuals that have administrative access to information. User permissions are reviewed regularly to ensure that users permissions are valid and that there are no Segregation of Duties (SOD) concerns.
All VRM IT employees that support the VRMS application have confidentiality agreements and NDA in place with VRM. The execution of these agreements is a prerequisite for working with client data.

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

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

All VRM personnel associated with the performance of VA contracted tasks, as well as Servicing and Originations personnel, are required to take "VA Privacy and Information Security Awareness and Rules of Behavior" training annually, such training is tracked and enforced, and access to VA data is removed for anyone failing to take such recurring training timely. Additionally, all VRM personnel are required to take VRM's internal IT Policy & Privacy training annually; such training is tracked and enforced.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 03/30/2023

3. *The Authorization Status:* Authorized to Operate (ATO)
4. *The Authorization Date:* 12/10/2020
5. *The Authorization Termination Date:* 12/10/2023
6. *The Risk Review Completion Date:* 12/03/2020
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* MODERATE

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.***

Not applicable.

Section 9 – Technology Usage

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

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

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

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

Yes, VA Partial Claims application is hosted in the Microsoft Azure cloud.

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.*

Based on the Microsoft Online Subscription Agreement, VRM owns and is solely responsible for data managed by VRM (including VA data) stored in the Azure Cloud. Reference: https://azure.microsoft.com/en-us/support/legal/subscription-agreement/

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.

Microsoft acquires no rights in Customer Data or Professional Services Data, other than the rights VRM grants to Microsoft. VRM has authorized Microsoft to collect information regarding VRM's use of Azure's cloud services (usage statistics, billing information, etc.). There is no collection of ancillary data in relation to VRM's data (including VA data) or the processing of that data.
Please see the sections: "Nature of Data Processing; Ownership" and "Processing for Business Operations: in Microsoft Products and Services Data Protection Addendum cited below.
Reference: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?isToggleToList=True&lang=1

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.

Yes. Based on the Microsoft Online Subscription Agreement, VRM owns and is solely responsible for data managed by VRM (including VA data) stored in the Azure Cloud. VRM has the sole ability to access, configure, and administer data and services in the Azure Cloud. VRM is accountable for implementing and maintaining privacy protections and security measures to safeguard data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed. These measures are outlined in a VRM's security policies.

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).

VRM does not utilize Robotic Process Automation (RPA) to process VA data.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

CHIQUITA DIXSON

Digitally signed by CHIQUITA DIXSON
Date: 2023.08.30 06:39:32 -04'00'

Privacy Officer, Chiquita Dixson

ANITA FEIERTAG

Digitally signed by ANITA FEIERTAG
Date: 2023.08.29 12:43:56 -04'00'

Information System Security Officer, Anita Feiertag

BERLETNEY HOUSE

Digitally signed by BERLETNEY HOUSE
Date: 2023.08.29 13:15:10 -04'00'

Information System Owner, Berletney House

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