Privacy Impact Assessment for the VA IT System called:

VA Loan Electronic Reporting Interface – Reengineering (VALERI-R)

Loan Guaranty (LGY) - Veterans Benefits Administration (VBA)

Date PIA submitted for review:

2/18/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Chiquita Dixon	Chiquita.Dixson@va.gov	202-632-8923
Information System Security Officer (ISSO)	Jason Beard	Jason.Beard@va.gov	512-326-6308
Information System Owner	Jose Corona	Jose.Corona@va.gov	727-502-1318

Abstract

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

VA Loan Electronic Reporting Interface Reengineering (VALERI-R) is a refactoring and modernization of the original VA Loan Electronic Reporting Interface (VALERI) system, which was conceptualized to enable Loan Administration (LA) to improve services to Veterans, oversight capability over Department of Veterans Affairs (VA) loan servicers and reducing the cost to the Government for defaulted loans. VALERI supports VA and VA Loan Guaranty's (LGY) mission in helping Veterans and their families retain their homes. VALERI is a web-enabled rules-based solution, designed to improve VA's oversight capability and to reduce the cost to the Government for the servicing and liquidation of VA-Guaranteed loans. It provides an interface between VA and the mortgage servicing community, allowing mortgage servicers to report significant event updates to VA focusing on default, loss mitigation, foreclosure, and claim payments. The current VALERI system provides both a web-interface and an integration component to allow automated loading of updates from VA mortgage servicers. The web-interface allows VAs technicians to manage VA loans and evaluate servicer performance, allowing VA to intervene on the Veteran's behalf, when necessary.

Overview

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

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

The VALERI-R project was conceptualized to modernize the legacyVALERI system, which enables VA to improve services to Veterans, improve oversight capability over VA loan servicers, and reduce the cost to the Government for defaulted loans. VALERI-R supports VA and LGYs mission in helping Veterans and their families retain their homes. VALERI-R system provides both a web-interface and an integration component to allow automated loading of updates from VA mortgage servicers. The web-interface allows VAs technicians to manage VA loans and evaluate servicer performance, allowing VA to intervene on the Veteran's behalf, when necessary. VALERI-R will have approximately 2.5 million VA loan records, which contain the personal financial data required to receive VA loans for Veterans and their co-borrowers.

VA uses VALERI-R to monitor the servicing of VA loans, generate loss mitigation recommendations, review adequacy of servicing, review non-routine claims and incentives, and conduct post-audits. VALERI-R also houses reporting and analytics tools for servicers and VA personnel. VALEI-R contains PII/SPI, in its Production and Pre-Production environments which are included in the VALERI-R Authorization Boundary. VALERI-R has the ability to generate reports which may contain data that has PII. This purpose is consistent with 5 U.S.C 5514, 4 CFR 102.5, and section 206 of Executive Order 11222 of May 8, 1965 (30 FR 6469). This purpose is consistent with the Federal Claims Collection Act of 1966 (Pub. L. 89-508, 31 U.S.C. 951-953 and 4 CFR parts 101-105), and the disclosure is authorized by 38 U.S.C. 3301(b)(6). Disclosure is consistent with 38 U.S.C. 3301(b)(6). Any information in this system may be disclosed to a State or municipal court or a party in litigation; or to a State or municipal grand jury, a State or municipal administrative agency functioning in a quasi-judicial capacity or a party to a proceeding being conducted by such agency, in order for the VA to respond to and comply with the issuance of a State or municipal subpoena; provided, that any disclosure of claimant information made under this routine use must comply with the provisions of 38 CFR 1.511.

Any information in this system, except for the name and address of a Veteran, may be disclosed to a Federal agency for the VA to obtain information relevant to the making, insuring, or guaranteeing of a loan under chapter 37 of title 38 U.S.C. The name and address of a Veteran may be disclosed to a Federal agency under routine use if they are required by the Federal agency to respond to the VA inquiry. **Note**: VALERI-R's authority to use PII data is established under the System of Records Notice (SORN) *55VA26: Loan Guaranty Home, Condominium and Manufactured Home Loan Applications Records, Specially Adapted Housing Applicant Records and Vendee Loan Applicant Records, VA.*

Veterans can request to review their information for accuracy by contacting the VA Regional Loan Center Responsible for their area. VALERI-R may share and receive privacy data with both VA systems and external VA loan servicers such as banks and credit unions. Individuals who have access to this data are authorized by the VA via the VA's elevated privileges process for individuals with system-level access for maintenance activities such as system administration, deployments, and troubleshooting. Users such as servicers and loan technicians with access to PII data via the front-end user interface will also be granted authorization by VA.

Additionally, the VA's origination system (Web LGY) sends social security number (SSN) and Military Service Number to VALERI-R, which are not stored as plaintext but rather hashed data. Once the hashed data is received, it does not decrypt nor repurpose it, but rather use it to compare a hashed value from within VALERI-R which corresponds to an SSN.

The Digital Transformation Center (DTC) Salesforce and Veterans Affairs Enterprise Cloud (VAEC) Amazon Web Services (AWS) GovCloud environments host the production version of VALERI-R, which contains PII data as it relates to VA home loans. These environments are FedRAMP compliant cloud platforms that provide Software, Platform, and/or Infrastructure as a Service (SaaS/PaaS/IaaS) for VALERI-R; these two environments have both been issued an authority to operate (ATO) by VA.

Section 1. Characterization of the Information

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

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

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

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

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

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

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

Financial Data

Other type of PII are VA Loan Numbers and Military Service Number.

PII Mapping of Components

VALERI-R consists of **2** key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **VALERI-R** and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

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

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Prod-Oracle RDS	Yes	Yes	Name, Social Security Number, Personal Mailing Address, Personal Phone Number, Emergency Contact Information, Financial Account Information, Race/Ethnicity, VA Loan Number, Military Service Numb	Provide analysis of VA Loans.	Data at rest encryption (disk/volume-level in place). Application-level encryption (Oracle Transparent Data Encryption-TDE).
Prodmirror-Oracle RDS	Yes	Yes	Name, Social Security Number, Personal Mailing Address,	Required for financial institution to upload VA Loan servicer files.	Data at rest encryption (disk/volume-level in place).

			Personal Phone Number, Emergency Contact Information, Financial Account Information, Race/Ethnicity, VA Loan Number, Military Service Number		

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

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

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

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

VALERI-R does not collect information from individuals. The PII data elements that are collected originate from VA home loan servicers and VA home loan servicer technicians. Veterans provide this information to the VA loan servicers when applying for a VA home loan. The VA's origination system sends encrypted Social Security Number & Military Service Number to VALERI-R, which are not stored as plaintext but rather hashed data. Executive Order 9397 (VA statute) requires the head of any Federal department or agency, to provide information, including SSNs, to the VA for purposes of determining eligibility for or amount of VA benefits, or verifying other information with respect thereto. VA loan information is transferred to the VA via an encrypted Secure File Transfer Protocol (SFTP) connection and stored on encrypted disk volumes.

1.3 How is the information collected?

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

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

Information is received by loan technicians. The loan servicers (such as PennyMac, First Bank of Omaha, etc.) provide the servicer files via an encrypted connection to a VALERI-R SFTP server or through the servicer web portal into VALERI-R and then VALERI-R transmits the data to the VA property management system.

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

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

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

VALERI-R provides a reporting mechanism to VA loan servicers and the VA. The VA verifies the Veteran's qualification by pulling in data from VA Defense Identity Repository (VADIR). The VA also provides a data quality team to reaffirm the accuracy of the information. VA loan servicers continually check the validity of the data they are sending to the VA before the information is used to make decisions about a particular Veteran's home loan, which protects against instances of data corruption, whether intentional or unintentional. To minimize risk, access is based on Role-Based privileges. All internal employees and contractors with access to Veteran's information are required to have the appropriate level background investigation and must complete the VA Privacy and Information Security Awareness training and Rules of Behavior (ROB) annually. To access into the VA network before access to Veteran's data, privileged members/contractors go through multi-factor authentication. The user ID limits the access to only the information required to enable the user to complete their job. The cloud components of this system are FedRAMP certified and will provide additional means to ensure data integrity and accuracy once the high availability infrastructure has been stood up.

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

SORN 55VA26, Executive Order 9397 (VA statute) requires the head of any Federal department or agency, to provide information, including SSNs, to the VA for purposes of determining eligibility for or amount of VA benefits, or verifying other information with respect thereto.

Title 38 U.S.C. § 5106 (VA statute) requires the head of any Federal department or agency, including SSA, to provide information, including SSNs, to the VA 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. Veteran SSNs are used to validate eligibility requirements and rating information from the external systems. SORN 55VA26: Loan Guaranty Home, Condominium and Manufactured Home Loan Applicants Records, Specially Adapted Housing Applicant Records and Vendee Loan.

1.6 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

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

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

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

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

<u>Principle of Data Quality and Integrity:</u> 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: VALERI-R supports the VA and LGY loan guarantee by providing both a web-interface and an integration component to allow automated loading of updates from VA mortgage servicers. VALERI-R requires collecting the personal financial data of Veterans and their co-borrowers. The largest privacy risk to the individual whose records are retained by VALERI-R would be a data breach, which may result in sensitive information such as home address, income, financial status, employment, etc. being exposed and having the potential to be exploited for any number of reasons, including financial gain. The privacy data collected by VALERI-R is necessary to support the VA's Loan Guaranty program. Accurate, detailed information about active and legacy loan data provide LGY the ability to make informed decisions for the core mission of the Loan Guaranty program: helping Veterans and their families retain their homes by improving VA loan services, improving oversight over VA loan servicers, and reducing the cost to the Government for defaulted loans. The information being collected is necessary in order to effectively facilitate decisions on VA loans.

VALERI-R does not collect any PII data directly from individuals. This is due to the way that VA loans are provided to Veterans, directly through loan servicers such as banks and credit unions which conduct business with Veterans. The VA does not have the capability to service loans for Veterans. VALERI-R is provided loan information directly from servicers, who are responsible for maintaining accurate, complete, and current information about VA loans. Veterans' eligibility status is the responsibility of the VA and is facilitated by the Veteran demographic data maintained in the VADIR. VALERI-R will also utilize previously collected PII data for Analytics purposes.

Mitigation: The risk of a data breach where information and systems are compromised is mitigated in several ways. Mitigations include requiring authentication and authorization to access the VALERI-R application and to see certain loan records. Loan servicers are limited to viewing records for loans for which they are the sole servicer. They are not allowed to view any information about loans which are not within their scope to service. Logging into the VALERI-R application requires a loan servicer technician to register with a ID.me credential, which is VA Identity and Access Management (IAM)-approved identity provider, VALERI-R inherits the ID.me solution from VA IAM, which has several validation procedures to ensure that an individual registering for a credential is who they claim to be.
VALERI-R adheres to information security requirements instituted by the VA 6500 handbook and other Federal government security directives. The VALERI-R project works with the assigned Information System Security Officer (ISSO) to continually determine how best to comply with security requirements. Access controls like role-based access are in place to prevent misuse. VALERI-R operates in two FedRAMP approved, VA-specific cloud environments: Salesforce for the user-interface and its associated infrastructure and AWS GovCloud for the rest of the back-end infrastructure, including the VALERI-R Oracle database and the VALERI-R Simple Storage Service (S3) instance. The PII data collected and stored for VALERI-R is encrypted at rest in the VA Salesforce instance by leveraging the Salesforce SHIELD platform. The SHIELD platform provides the VA with additional security capabilities beyond what is available in standard Salesforce deployments. These items include Federal Information Processing Standards (FIPS) 140-2 encryption of all data, data elements, files, notes, etc. stored in the Salesforce environment regardless of size or filetype.

The VA AWS GovCloud environment provides numerous protections as access to VALERI-R environments requires being on the VA network, VA credentials with VALERI-R VA System Owner-approved elevated privileges, and access approved and provisioned by the VA Enterprise Cloud team. The VA instance of GovCloud provides VALERI-R with FIPS 140-2 compliant encrypted disk volumes, using the Red Hat Linux (RHEL) operating system which has been secured by the VA according to the VA RHEL baseline configuration guide, so all PII data stored on VALERI-R systems is encrypted by default and is utilized by VALERI-R system components using a VA secured operating system. Additionally, PII data stored within the VALERI-RRDS database will be secured within the database itself using Transparent Data Encryption (TDE) capability. TDE will provide an additional layer of protection for PII data if a breach occurs, despite the above listed risk mitigations efforts, and unauthorized individuals gain access the server where the database resides. Lastly, PII data stored within the VALERI-R S3 instance, which is by default secured in the AWS GovCloud environment using FIPS 140-2 compliant encrypted disk volumes using AES-256 encryption.

Training is provided to all internal employees with access to Veteran's information, such as the VA Privacy and Information Security Awareness training. Users with privileged access are required to take elevated privilege training via the VA Training Management System (TMS). Additionally, the risk of lost or stolen PII can result in fines (per record) to the organizations responsible for maintaining such data, and in some cases a loss of contract if a contracting organization is determined to be responsible for the breach.

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.

The privacy information in VALERI-R will be used to support Loan Administration (LA) in improving services to Veterans, improve oversight capability over VA loan servicers, and reduce the cost to the Government for defaulted loans. VALERI-R supports VA and VA Loan Guaranty's (LGYs) mission in helping Veterans and their families retain their homes. VALERI-R system provides both a web-interface via SalesForce and an integration component to allow automated loading of updates from VA mortgage servicers. The web-interface allows VAs technicians to manage VA loans and evaluate servicer performance, allowing VA to intervene on the Veteran's behalf, when necessary. VALERI-R will have approximately 2.5 million VA loan records, which contain the personal financial data required to receive VA loans for Veterans and their co-borrowers.

The SalesForce platform handles the data used for case management and claims processing. Name and social security numbers are used to identify and track individual(s) in VA systems. The address is needed so that VA can send correspondence to Veterans. Military service and active-duty separation information (e.g., name, service number, race/ethnicity, email address, date of birth, rank, total amount of active service, branch of service, character of service, pay grade, assigned separation reason, service period, whether Veteran was discharged with a disability, reenlisted, received a Purple Heart or other military decoration) is used to verify the Veteran's service information. Payment information (e.g., Veteran payee name, address, dollar amount of readjustment service pay, amount of disability or pension payments, any amount of indebtedness (accounts receivable) arising from title 38 U.S.C. benefits and which are owed to the VA) is kept for record purposes only.

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

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

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

Utilizing a combination of known information about the Veteran and the VA loan associated with that individual, VALERI-R will provide actionable analytics to help Veterans retain their homes.

VALERI-R leverages the Salesforce platform to perform analytics using Einstein (Cloud based system checks, identifying patterns and managing a mostly automated system). The platform serves as means of reporting back on possible actions regarding an individual's loan. VALERI-R also utilizes Microsoft's PowerBI platform in order to generate reports, dashboards and analytics graphsto enhance LGY's reporting capability. This analytics data currently resides in VALERI-R to support VA loan technicians and other stakeholders. The Analytics capability is being stood up as a separate information system that is in its development and authorization process. In the future, VALERI-R will be providing its data to the LGY Analytics (LGA) information system for those same purposes.

2.3 How is the information in the system secured?

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

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

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

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

VALERI-R secures data by providing both encryption of data in transit using the SFTP protocol for large file transfers from servicers and SSL certificates for communications between the VALERI-back-end and the Salesforce front-end application. Encryption of data at rest includes the use of Salesforce Shield encryption, AWS KMS encryption for data stored in the VAEC AWS GovCloud and Oracle Transparent Data Encryption (TDE) for all VALERI-R Oracle databases.

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

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

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

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

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

Access is assessed based on Role-Based privileges. All internal employees and contractors with access to Veteran's information are required to have the appropriate level background investigation and must complete the VA Privacy and Information Security Awareness training and ROB annually. To access into the VA network before access to Veteran's data, privileged members/contractors go through multi-factor authentication. Contractors are given access to Veteran's data and to only the information required to enable the user to complete their j. The

cloud components of this system (Salesforce and AWS GovCloud) are FedRAMP certified and have been issued Authority to Operate by the VA.

External users are vetted through their lender/servicer organization. An administrator within the servicer organization authorizes the initial user registration and then validates their continued access every 90 days.

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

- Name
- Service Information
- Loan Information
- SSN
- Date of Birth
- Mailing address and ZIP code
- Phone Number(s)
- Financial Account information
- Race/Ethnicity
- Emergency Contact

3.2 How long is information retained?

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

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

Individual Veteran's file folders, claims records, and loan information (Operational data) is accessible through VALERI-R's utilization of the SalesForce platform for 2 years, as well as

said Veteran's information is additionally retained at the servicing regional office for the life of the Veteran. At the death of the Veteran, these records are sent to the Federal Records Center (FRC), maintained by the FRC for 75 years, and thereafter destroyed at the direction of the Archivist of the United States. The Veterans' records are not eliminated but are stored either on tape or disk indefinitely (VA SORN 55VA26 Loan Guaranty Home, Condominium and Manufactured Home Loan Applicants Records, Specially Adapted Housing Applicant Records and Vendee Loan Applicant Records VA Having access to legacy loan data supports LGY's mission as a key component of ongoing analytics being performed to best support Veterans in retaining their homes.

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

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

The retention schedule has been approved by the National Archives and Records Administration (NARA) and can be found at Veterans Benefits Administration Records Management, Records Control Schedule VB–1, Part 1, Section XII (Loan Guaranty) (https://www.benefits.va.gov/WARMS/docs/regs/RCS_I.doc).

3.4 What are the procedures for the elimination of SPI?

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

Individual Veteran's file folders, claims records, and loan information accessible through VALERI-R are retained at the servicing regional office for the life of the Veteran. At the death of the Veteran, these records are sent to the Federal Records Center (FRC), maintained by the FRC for 75 years, and thereafter destroyed at the direction of the Archivist of the United States. Electronic data and files of any type, including PII and Sensitive Personal Information (SPI), are destroyed in accordance with the Department of Veterans' Affairs Handbook 6500.1, Electronic Media Sanitization (November 3, 2008), http://www.va.gov/vapubs/viewPublication.asp?Pub_ID=416&FType=2. When required, this data is deleted from their file location and then permanently deleted from deleted items folders. Magnetic and digital media used to support VALERI-R is wiped or shredded and sent out for

destruction per VA Handbook 6500.1 as detailed in the respective system security plans for VAEC AWS GovCloud and Salesforce.

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

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

Currently, there is no active PII used in testing, training or research as de-identified or dummy PII being used. If PII is needed for testing, it will only reside within the VA Salesforce and AWS GovCloud environments, and under VA provided privacy controls and processes. PII will not be used for research or training purposes.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

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

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

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

Follow the format below:
Privacy Risk: VALERI-R will only retain the information needed to support the mission of the VA and its Loan Guaranty program. PII that's collected will be retained within VALERI-R for the duration of the VA loan and remains relevant once the VA loan is inactive for analytics

purposes. Due to the analytics that VALERI-R will provide based on current and inactive loan data, there are no plans to purge data. There is a risk that data may be assessable to unauthorized persons in the event that there is a successful data breach of VALERI-R.

Mitigation: The only current mitigation to this risk is for VALERI-R to continue to apply all security measures to the data it stores, indefinitely. VALERI-R applies data at rest encryption of all storage volumes and will continue to do so indefinitely. VALERI-R will also continue to apply all Access Controls to prevent access to VALERI-R data by unauthorized individuals.

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***
WebLGY	WebLGY connects VALERI-R with other VA LGY systems involved in the loan guaranty process. WebLGY will need to temporarily provide current VA loan data required for operation.	Initial based VA loan information, updates, and current VA loan data.	Electronically – XML files inbound/outbound via Simple Object Access Protocol (SOAP)
The Appraisal System (TAS)	Loan appraisal information required as part of the analytics being performed on VA loans.	Loan Appraisal information	Electronically: flat files via SOAP
Property Management (CPTS)	Property and loan status information is required as part of the analytics being performed on VA loans	VA loan and property status information	Electronically via XML file exchange
Financial Management System (FMS)	Loan payment status information is required as part of the analytics being performed on VA loans.	Payments and other accounting transactions	Electronically via flat files inbound/outbound
Stakeholder Information Management (SIM)	Loan appraisal and builder information is required as part of the analytics being performed on VA loans.	Loan appraisal and builder data.	Electronically – XML files via SOAP
Identity and Access Management (IAM)	Servicer technicians and loan technician's identity information that is required to	Identity information for VALERI-R users	Electronically

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*
	ensure that only authorized individuals are accessing the system.		
LGY Document Store	Loan documentation is required to be stored in a LGY managed environment. The VALERI-R database cannot store artifacts such as documents or spreadsheets	Loan documentation	Electronically via an Application Programming Interface (API)
VA/DoD Identity Repository (VADIR)	Veteran demographic information is required as part of the overall data analytics capability.	Veteran demographics and other associated VA data	Electronically via SOAP requests/responses
Performance Analysis & Integrity (PA&I)	Loan performance and integrity is required as part of the analytics being performed on VA loans.	PA&I Accuracy and Non-Accuracy data	Electronically via flat files
ServiceNow (SNOW)	For the purposes of entering service desk tickets in order to provide support to VALERI-R users	Name, username, e-mail address, phone number, role type, affiliate ID	Electronically
Loan Guaranty Analytics (LGA)	VA loan information.	Name, Social Security Number, Personal Mailing Address, Personal Phone Number, Emergency Contact Information, Financial Account Information, Race/Ethnicity, VA Loan Number, Military Service Numb	Electronically using a SSL connection to the LGA Syst

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

Follow the format below:
Privacy Risk: The primary risk with sharing this information within the VA would be a case where another VA system that VALERI-R will send data to is not able to have the appropriate security policies and procedures in place, such as disk/volume-level encryption.

Mitigation: Training is provided to all project employees. All personnel with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and ROB annually. Additionally, VALERI-R adheres to all VA information security requirements instituted by the VA Office of Information Technology (OIT). Users can only access VA sensitive data and PII within the VA network, as well as, no sensitive/PII/data can be transmitted outside the VA network. Risks that are specific to the individual application that sends/receives data from VALERI-R are not able to be mitigated as this is outside scope of the VALERI-R project.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
Arvest Mortgage	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
BankPacific	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
Black Knight Servicing Technologies, LLC	Veteran Loan Information	PII	Signed MOU/ISA in place – Revisions requires, renewal in progress	Inbound data transfer via SFTP
Brand Mortgage	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
CIS Financial Services Inc	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
Corning Credit Union	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
DHI Mortgage	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP

Elmira	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
ENT Credit Union	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
Envoy Mortgage	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
First National Bank of Omaha	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
FirstLight Credit Union	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
Flat Branch Mortgage, Inc	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
Gateway Mortgage	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
GTE Federal Credit Union	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
Guardian Mortgage	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
Guild Mortgage	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
Hudson Valley CU (formerly Hudson Valley Federal Credit Union)	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
Idaho Housing and Finance	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
Intercap	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
Kentucky Housing	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
Kirtland	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP

Kondaur Capital	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
McDonald Computer Corp System (Sunwest)	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
Midfirst Bank	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
Mortgage Builder	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
MR.COOPER/Nationstar	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
New Rez (Shellpoint)	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
North Dakota Housing	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
Northwest FCU	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
Oriental Bank	Veteran Loan Information	PII	Signed MOU/ISA in place – Revisions requires, renewal in progress	Inbound data transfer via SFTP
PennyMac Loan Svc	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
Pulte Mortgage	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
Rocky Mountain	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
Sagent M&C, LLC (formerly Fiserv)	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
Selene	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP

Service Credit Union	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
SN Servicing	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
Standard Mortgage	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
TN Housing (Tennessee Housing Development Agency)	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
Town and Country	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
Trustmark	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
TTCU	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
University Bank/Midwest	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
VEROS	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
Veterans Home Purchase Board of MS	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
Weststar Mortgage Corp	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
Fortera Credit Union	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP
Wyoming Community Development Authority	Veteran Loan Information	PII	Signed MOU/ISA in place	Inbound data transfer via SFTP

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 privacy risk for external information sharing is that external entities such as servicers may not necessarily provide the level of care of the data once they receive it from VALERI-R. There are not contractual obligations for servicers to appropriate protect Veteran's data, just MOUs.

Mitigation: MOUs approved all Loan Servicers listed on the table above. These MOUs which include a section covering methods used by the parties to secure data, are vetted and signed by parties on the external servicer side and the VA system owner and ISSO.

Section 6. Notice

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

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

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

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

Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

This does not apply to VALERI-R as it does not collect data directly from individual Veterans. VA loan servicers are responsible for providing these notices to Veterans during the loan origination. SORN 55VA26 Loan Guaranty Home, Condominium and Manufactured Home Loan Applicants Records, Specially Adapted Housing Applicant Records and Vendee Loan Applicant Records VA. https://www.oprm.va.gov/docs/Current_SORN_List_06_25_2021.pdf).

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

Not applicable to VALERI-R as Veterans do not interact with VALERI-R, individuals have the right to decline to provide their information to the lender; however, without providing the information the lender cannot originate a VA Home 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

Not applicable to VALERI-R as Veterans do not interact with VALERI-R. The Veteran provides consent for the lender to use the information by originating the VA Home Loan, and the subsequent servicing of the loan.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.

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

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

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

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

Follow the format below:
Privacy Risk: This does not apply to VALERI-R as Veterans do not interact with VALERI-R. No risks related to providing insufficient notice as Veteran's are aware of their provision of consent for the lender to use the information by originating the VA Home Loan, and the subsequent servicing of the loan.

Mitigation: Not Applicable.

Section 7. Access, Redress, and Correction

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

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

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

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

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

Veterans are provided disclosures during the time of loan origination, which is a process that the Veteran themselves initiate. Procedures detailed from VA Handbook 6300.4:
(1) An individual may request amendment of a record pertaining to him or her contained in a specific VA system of records by mailing or delivering the request to the office concerned. The request must be in writing and must conform to the requirements in paragraph 3b(3) of this handbook. It must state the nature of the information in the record the individual believes to be inaccurate, irrelevant, untimely, or incomplete; why the record should be changed; and the amendment desired. The requester should be advised of the title and address of the VA official who can assist in preparing the request to amend the record if assistance is desired.

(2) Not later than 10 days, excluding Saturdays, Sundays, and legal public holidays, after the date of receipt of a request to amend a record, the VA official concerned will acknowledge in writing such receipt. If a determination has not been made, the acknowledgement will inform the individual when he or she may expect to be advised of action taken on the request. VA will complete a review of the request to amend or correct a record as soon as reasonably possible, normally within 30 days from receipt of the request (excluding Saturdays, Sundays, and legal public holidays)
(3) Where VA agrees with the individual's request to amend his or her record(s), the requirements of 5 U.S.C. 552a(d) will be followed. The record(s) will be corrected promptly, and the individual will be advised promptly of the correction. Amendment consists of adding information to the record, altering information in the record, or deleting information in the record. Under the Privacy Act, if information is altered or deleted, the previous version must be obliterated and illegible after amendment. The amendment should be annotated "Amended, Privacy Act, (date), (signature and title of amending official)."
(4) If the record has previously been disclosed to any person or agency, and an accounting of the disclosure was made, prior recipients of the record will be informed of the correction. FL 70- 19, Notification to Other Person or Agency of Amendment to a Record, may be used.
(5) If it is determined not to grant all or any portion of the request to amend a record, the official will promptly notify the individual in writing. The individual will be advised of his or her right to file a concise statement of reasons for disagreeing with the refusal to amend. The notice will specify the reason(s) for denying the request, identify the VA regulations or statutes upon which the denial is based, and advise that the denial may be appealed in writing to the General Counsel (024), VA, 810 Vermont Avenue, NW, Washington, DC 20420. FL 70-20, Notification of Initial Refusal to Amend a Record Under the Privacy Act, may be used for this purpose.
(6) The determination on an appeal will be made not later than 30 days, excluding Saturdays, Sundays, and legal public holidays, from the date the individual's letter of appeal is received unless the Secretary or Deputy Secretary, for good cause shown, extends such 30-day period. If the 30-day period is so extended, the individual will be notified promptly of the reasons for the extension and the date on which a final determination may be expected. The final determination in such appeals will be made by the General Counsel or Deputy General Counsel.
(7) If the General Counsel or Deputy General Counsel finds that the adverse determination should be reversed, he or she will notify the VA office or station of the remedial action to be taken. The VA
office or station will promptly carry out that action. The General Counsel or Deputy General Counsel will promptly notify the individual in writing of the corrective action. The field station or Central Office organization that provided the initial decision will inform previous recipients of the record that a correction has been made.
(8) If the General Counsel or Deputy General Counsel determines that the adverse determination will not be reversed, the individual will be notified promptly in writing of that determination, the reasons therefor, and of his or her right to seek judicial review of the decision pursuant to section 3 of the Privacy Act (5 U.S.C. 552a(g)). Version Date: January 10, 2019 Page **21** of **27**
(9) If the adverse determination is sustained by the General Counsel or Deputy General Counsel, the individual will also be advised promptly of his or her right to file a concise statement of reasons for disagreeing with the refusal to amend. The statement may contain information that the individual believes should be substituted.

(10) When an individual files a statement disagreeing with VA's decision not to amend a record, the record will be clearly annotated so that the fact that the record is disputed is apparent to anyone who may subsequently access, use, or disclose it. When the disputed record is disclosed to persons or other agencies, the fact of the dispute will be clearly noted. Copies of the statement of disagreement will be provided, and, when appropriate, copies of a concise statement of VA's reasons for not making the amendment(s) requested will also be provided.
(11) A decision by either the General Counsel or Deputy General Counsel pursuant to paragraph 3f(7) of this handbook is final. It is subject to judicial review in the district court of the United States in which the complainant resides, or has his or her principal place of business, or in which the VA records are located, or in the District of Columbia.

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.

As directed in VA SORN 55VA26, the lender must log on to the system using the unique 10-digit lender identification number assigned by VA and a unique password. The lender also must enter information identifying the specific Veteran, for whom the Interest Rate Reduction Refinance Loan (IRRRL) lender seeks information, including the Veteran's name, social security number and other identifying information, such as the 12-digit loan number for the Veteran's current VA-guaranteed loan or the month and year of the loan.
Veterans can request to review their information for accuracy by contacting the VA Regional Loan Center Responsible for their area, which is done through the FOIA (Freedom of Information Act) process, but contact information is not directly provided for a particular individual. Resolving erroneous information for the loan itself must go through the loan servicer. This information is relayed during the loan origination process directly with the lender.

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Individuals are notified via a VA Release Form of how to correct their information by the lender.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

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

No alternatives are provided. The Veteran and lender work together to gather all of the information. Once all information is gathered, and supporting documentation verified, a final version of the Veteran's loan application is created. This includes all corrections that were made as part of the loan application and approval process. A closing agent reviews all of the documentation with the Veteran and obtains the Veteran's signature that the information is correct. Data entry errors after the fact are corrected by the multiple layers of lender internal audits, and VA audits conducted.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

Principle of Individual Participation: If access and/or correction is denied, then is the individual provided notice as to why the denial was made and how to challenge such a denial?

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?
This question is related to privacy control IP-3, Redress.

Follow the format below:
Privacy Risk: VALERI-R does not provide individual access to the system, which may carry the risk of inaccurate data.

Mitigation: Veterans do not have access to the VALERI-R system to obtain their information. However, VA employees can access their information, but this will soon be phased out. If a Veteran request their information, it is done through the FOIA (Freedom of Information Act)

process, but contacts are voided from the granted information. Veterans can request to review their information for accuracy by contacting the VA Regional Loan Center Responsible for their area VALERI-R will share and receive privacy data with both VA systems and external VA loan servicers such as banks and credit unions. Individuals who have access to this data will be authorized by the VA via the VA's elevated privileges process for individuals with system-level access for maintenance activities such as system administration, deployments, and troubleshooting. Users such as servicers and loan technicians with access to PII data via the front-end user interface will also be granted authorization by the VA.

Section 8. Technical Access and Security

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

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

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

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

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

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

All internal employees and contractors with access to Veteran's information are required to have the appropriate level background investigation and must complete the VA Privacy and Information Security Awareness training and ROB annually. To access into the VA network before access to Veteran's data, privileged members/contractors go through multi-factor authentication. Contractors are given access to Veteran's data through the issuance of a user ID and password. This ensures the identity of the user by requiring two-factor authentication. The user ID limits the access to only the information required to enable the user to complete their job. The cloud components of this system are FedRAMP certified and will provide additional means to ensure data integrity and accuracy once the high availability infrastructure has been stood up. Technicians from loan servicers are reviewed and approved by the VA prior to onboarding to use VALERI-R.

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 who have privileged access will have access to the development side of the system. The contractors will have complete involvement in the design and maintenance of the system, until migration into production. NDAs are part of the contractual agreement between the contractor and the VA All internal employees and contractors with access to Veteran's information are required to have the appropriate level background investigation and must complete the VA Privacy and Information Security Awareness training and ROB annually. To access into the VA network before access to Veteran's data, privileged members/contractors go through multi-factor authentication. The user ID limits the access to only the information required to enable the user to complete their job. The cloud components of this system are FedRAMP certified and will provide additional means to ensure data integrity and accuracy.

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.

Contractors are required to take the VA privacy security training. Additional security awareness training is provided once during on-boarding and semi-annually by the VALERI-R project, which also details how to handle PII/Sensitive information. All individuals are also required to take the VA TMS HIPPA annual training.

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

If Yes, provide:

1. *The Security Plan Status,*
2. *The Security Plan Status Date,*
3. *The Authorization Status,*
4. *The Authorization Date,*
5. *The Authorization Termination Date,*

6. *The Risk Review Completion Date,*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

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

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

1. Security Plan status: Completed
2. Security Plan Status date: June 25, 2021
3. Authorization Status: Full ATO
4. Authorization Date: August 26, 2021
5. Authorization Termination date: August 26, 2022
6. Risk Review completion date: July 30th, 2021
7. FIPS 199 Classification of the system: MODERATE/MODERATE/MODERATE

Section 9 – Technology Usage

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

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

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

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

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

The system utilizes Cloud technology, system is hosted on the VAEC AWS GovCloud which is FedRAMP authorized. VALERI-R's front-end uses Salesforce which is hosted by the DTC, also FedRAMP authorized. VALERI-R utilizes the Infrastructure as a Service (IaaS) and Software as a Service (SaaS) cloud models.

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

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

For all Cloud deployments in the VAEC, the customer (in this case VA and VALERI-R) owns the data and identities.
Source: https://dvagov.sharepoint.com/sites/OITECSO/SitePages/Cybersecurity-in-the-VAEC.aspx

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.

Per VAEC's Privacy Impact Assessment dated June 28, 2019 only system level audit logging is stored on the VAEC systems. Users access the VAEC via their VA Active Directory (AD) account. Data is only retained while the user has an account with VAEC and VAEC does not collect or maintain PII.

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.

This principle is described in the VAEC Cybersecurity website: https://dvagov.sharepoint.com/sites/OITECSO/SitePages/Cybersecurity-in-the-VAEC.aspx and also described in mor detail in the VAEC PIA which was approved on June 28, 2019.

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).

Not Applicable to the VALERI-R information system.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

Chiquita Dixson 126558

Digitally signed by Chiquita Dixson 126558
Date: 2022.03.02 14:23:51 -05'00'

Privacy Officer, Chiquita Dixon

Jason A Beard 202593

Digitally signed by Jason A Beard 202593
Date: 2022.03.02 11:24:02 -06'00'

Information Systems Security Officer, Jason Beard

Jose R. Corona 326783

Digitally signed by Jose R. Corona 326783
Date: 2022.02.28 06:34:38 -05'00'

Information Systems Owner, Jose Corona

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).

This does not apply to VALERI-R as it does not collect data directly from individual Veterans. VA loan servicers are responsible for providing these notices to Veterans during the loan origination. SORN 55VA26 Loan Guaranty Home, Condominium and Manufactured Home Loan Applicants Records, Specially Adapted Housing Applicant Records and Vendee Loan Applicant Records VA. https://www.oprm.va.gov/docs/Current_SORN_List_06_25_2021.pdf).