Privacy Impact Assessment for the VA IT System called:

Salesforce Veteran Home Benefits (VHB)

Veterans Benefits

Administration (VBA)

Loan Guaranty

eMASS ID 2454

Date PIA submitted for review:

6/13/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Chiquita Dixson	Chiquita.dixson@va.gov	804-638-4522
Information System Security Officer (ISSO)	Patrick Stanford	Patrick.stanford2@va.gov	254-709-8625
Information System Owner	Terrance Wilson	Terrance.wilson@va.gov	410-708-6471

Abstract

Salesforce Veteran Home Benefits (VHB) is a transformation effort to support the Loan Guaranty Program Office. VHB application's main goal is to provide eligibility verification for Veterans, Loan Guaranty Certificates to lenders, management of Real Estate Owned (REO) properties, and oversight for the Loan Guaranty program.

Overview

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

1 General Description

A. What is the IT system name and the name of the program office that owns the IT system?
Salesforce Veteran Home Benefits (VHB) – VBA – Loan Guaranty

B. What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?
Provide eligibility verification for Veterans, Loan Guaranty Certificates to lenders, management of Real Estate Owned (REO) properties, and oversight for the Loan Guaranty program. Overall purpose of the system will be to process and monitor VA home loans, including the public sell of some properties.

C. Who is the owner or control of the IT system or project?
VHB is hosted at the Salesforce GovCloud Plus and VAEC AWS GovCloud

2. Information Collection and Sharing

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

Eventually VHB will contain records for over 20 million users, the first components to go into production will contain approximately 1000 users and 18 million unique records.

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

The system collects, retrieves, stores, and disseminates Personally Identifiable information (PII) data for loan information.

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

VHB solution is going to replace the existing LGY Cloud Assessing system. VHB consists of an external Application Programming Interface (API) hosted in the Mulesoft DIP Platform cloud and a User Interface (UI) implemented in Salesforce. The API is the primary interface for loan industry users that includes lenders, servicers, appraisers, and veterans. Requests that come from the mortgage industry that cannot be automatedly processed will create a workflow for manual processing. Once the manual processing is completed, a response will be returned to the requester and captured as an action in UI. If a lender or servicer reports a loan in default, then the system will begin to manage that loan as a REO. A REO will incur costs and generate revenue until it is sold. The system aids in maintaining accurate information on the debits and credits related to each request. The actions performed in the UI will be recorded in the AWS hosted database used by the API which will remain as the authoritative data source in the system. The system derives information that is gathered from multiple data feeds within the LGY product line to process home loan benefits for eligible Veterans. Interfaces with other systems, which will be added in future versions, are varied including but not limited to, mortgage industry retrieving veterans' information to determine eligibility; financial systems to process collections and payments. VHB tool intends to provide regulatory oversight information to other government entities and exchange data with commercial systems contracted to handle an aspect of the program.

G. Is the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites?

N/A – system is not operated at multiple sites.

3. Legal Authority and SORN

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

The legal authority to operate system is Title 38 USC, 3700 et seq. and Title 38 USC, 2100 et seq: 38 USC, section 210©, and Chapters 11, 13, 15, 31, 34, 35, and 36, 38 USC, Chapter 3, section 21©(1): 38 USC, 1901 et.

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?

The SORN is in process of being updated. The SORN number is 55VA26 - Loan Guaranty Home, Condominium and Manufactured Home Loan Applicants Records, Specially Adapted Housing Applicant Records and Vendee Loan Applicant Records – VA.

4. System Changes

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

No business process will be changed due to the completion of this PIA.

K. Will the completion of this PIA could potentially result in technology changes?
No Technology changes will be made due to the completion of this PIA.

Section 1. Characterization of the Information

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

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

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

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

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. It must also match the information provided in question 3.4 of the PTA.

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

- ☒ 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[1]
- ☐ 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)

[1] *Specify type of Certificate or License Number (e.g., Occupational, Education, Medical)

☐Military History/Service Connection
☐ Next of Kin

☒ Other Data Elements (list below)

Other PII/PHI data elements: UserID, Username, Loan ID Number, loan payment amounts, Liquid assets value, FICO, Household income, Integration Control Number (ICN). Disability rating, Disability Percentage from VA, Purple heart recipient, Veteran's tours of duty including character of discharge.

PII Mapping of Components (Servers/Database)

VHB consists of 4 key components (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by VHB and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	**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**
LGY VAEC AWS RDS instance	**No**	**Yes**	*First Name, Last Name, Date of Birth (DOB), Social Security Number (SSN), Mailing Address, Personal Contact number, Personal email address, Race/ Ethnicity, Loan Information (loan id number, loan payment amounts) Financial account, Integration Control Number (ICN)*	**To determine eligibility**	**PII only accessed by authorized users with access to the system**
LGY Cloud Assessing	**No**	**Yes**	*Veteran Name, Date of Birth (DOB), Social Security Number (SSN), Mailing Address, Personal Contact number, Personal email address, Loan*	**To determine eligibility**	**PII only accessed by authorized users with access to the system**

			Information (loan id number, loan payment amounts)		
VHB VAEC AWS Amazon Aurora	**No**	**Yes**	*First Name, Last Name, Date of Birth (DOB), Social Security Number (SSN), Mailing Address, Personal Contact number, Personal email address, Race/ Ethnicity, Loan Information (loan id number, loan payment amounts) Financial account information, Integration Control Number (ICN)*	**To improve visibility to loan data to enhance the LGY program.**	**PII only accessed by authorized users with access to the system**
LGY AWS S3	**No**	**Yes**	*Veteran Name* *Date of Birth (DOB)* *Social Security Number (SSN)* *Mailing Address* *Personal Contact number* *Personal e-mail address* *Race/Ethnicity* *Loan Information, such as loan ID number, loan payment amounts* *Liquid assets value* *FICO* *Household income* *Integration Control Number (ICN)* *Disability rating* *Disability percentage from VA* *Purple heart recipient* *Veteran's tours of duty including character of discharge*	**To improve visibility to loan data to enhance the LGY program.**	**PII only accessed by authorized users with access to the system**

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?

VHB will obtain Personal Contact information, Service Information, and Rating Diagnostics from the applicant and from other sources such as Department of Veterans Affairs (VA) files, and Department of Defense (DoD) systems.

1.2b Describe why information from sources other than the individual is required? For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

Other data such as loan information is gathered for eligibility requirements and is required to determine eligibility.

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

The information system is listed under the overview section.

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?

Personal information is collected from the applicant or from end users on the veteran's behalf. VHB does not collect Veteran PII directly from Veterans. The information come indirectly to VHB from loan servicers and e-benefits. Service information is extracted from VA files, DoD Systems and from the veterans themselves. Loan information is collected from other government and commercial sources such as the VBA Corporate Database. VA Loan Electronic Reporting Interface (VALERI), VA/DoD Identity (VADIR), eBenefits, Financial Management System (FMS), LGY partners such as Lenders, Services and Appraisers and the Benefits Identification and Locator System (BIRLS).

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, what is the form's OMB control number and the agency form number?

This system is not subject to the Paperwork Reduction Act.

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.

VHB data collected by lenders, appraisers, inspectors, and property managers is used for the various VBA applications. This data is factored into various criteria for determining if the Veteran is eligible for Home

Loan Guaranty or Specially Adapted Housing benefits. All information received by VHB applications are validated to ensure the data is formatted properly and accurate.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

If data is obtained from multiple sources (Veteran tour data) then that data is crosschecked both by the systems as well as internal loan specialists.

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

Title 38 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. Veteran SSNs are used to validate eligibility requirements and rating information from the external systems. SORN: Loan Guaranty Home, Condominium and Manufactured Home Loan Applicants Records. Specially Adapted Housing Applicant Records and Vendee Loan Applicant Records-VA 55VA26 by the Privacy Act of 1974, 5 U.S.C. 552a€(4 6, 5 U.S.C. 552a®and OMB 59 FR 37906, 3791618, July 25, 1994.

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. (*Work with your System ISSO to complete this section)*

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: Sensitive Personal Information including personal contact information, service information and benefit information may be released to unauthorized individuals.

Mitigation: VHB adheres to the information security requirements instituted by the VA Office of Information Technology (OIT). All Internal employees with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior training annually.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
Name	File Identification purposes	Identification purposes
Date of Birth	File Identification purposes	Identification purposes
Social Security Number (SSN)	Identification and tracking	Identification and tracking
Mailing address	For sending correspondence	For sending correspondence
Personal phone number	Contact Information	contact information.
Personal e-mail address	Contact Information	contact information.
Race/Ethnicity	Statistical purposes	Statistical purposes
Loan Information	to determine eligibility	to determine eligibility
Financial Account	to determine benefit amounts	to determine qualification for loan
Integration Control Number (ICN)	to determine eligibility	No external use
User ID	File Identification purposes	File Identification purposes
Username	File Identification purposes	File Identification purposes
Loan information / Loan ID	File Identification purposes	File Identification purposes
Loan Payment Amounts	Identification and tracking	Identification and tracking
Liquid Assets Value	record purposes	record purposes
FICO	record purposes	record purposes
Household Income	record purposes	record purposes
Disability Percentage from VA	Verification purposes	Verification purposes
Purple Heart Recipient	Verification purposes	Verification purposes

Veteran's tours of duty/character of discharge	Verification purposes	Verification purposes

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?

All information retained in VHB systems is used to determine Veterans eligibility for Home Loan Guaranty and Specialty Adapted Housing benefits. Subsequently, data obtained from VA partners servicing the home loan guaranty program is utilized by both automated and manual reviews to ensure those partners are adhering to good lending practices when serving the Veteran. VA Regional Loan Center (RLC) staff and VBA VACO Monitoring Unit staff also conduct audits of the lenders loan files (which included auditing funding fee information) as part of ongoing lender and RLC quality audits.

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.

Letters to Veterans concerning the progress of their claim are generated periodically, as well as rating decisions and requests for additional information to substantiate the claim. These letters are generated electronically and printed on paper and mailed to the Veteran.

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?
All VHB data in transit is transmitted using SSL encryption. Data at rest is protected via Salesforce SHIELD encryption.

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

All VHB data is encrypted in transit with SSL encryption. Data at rest is protected via Salesforce SHIELD encryption.

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

All VA employees and contractors working with VHB are required to take VA Privacy and Rules of Behavior, which includes training on how to safeguard PII/PHI.

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?

All users must register to access VHB Salesforce front-end application. Internal users are validated using VA PIV Card/Active Directory, external users are validated using ID.me 3rd party authentication service. The data requests.

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

All of the VA privacy overlay security controls will all be applied to this system and documented in the Authorization to Operate (ATO). The following privacy controls have been applied to the VHB information system and will be assessed: AR (Accountability, Audit and Risk Management), AP (Authority and Purpose), DM (Data Minimization and Retention), DI (Data Quality and Integrity), IP (Individual Participation and Redress), SE (Security), TR (Transparency), and UL (Use Limitation).

2.4c Does access require manager approval?

Yes.

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

VA Employees and 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's user ID limits the access to only the information required to enable the user to complete their job.

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

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

The VHB Information System Owner is the individual who is ultimately responsible for assuring that safeguards are being implemented for all PII contained in the system. All internal employees and contractors with access to the system's PII are required to have the appropriate level of background investigation and must complete the VA Privacy and Information Security Awareness training as well as the Rules of Behavior training on an annual basis. VA employees and contractors are given access to Veteran's data through the issuance of user accounts that require two-factor authentication. Salesforce GovCloud Plus, which is the VHB Cloud Service Provider is FedRAMP certified and has been issued Authority to Operate by the VA.

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*

VHB will store the primary subject's personal information, which will be retained after collection. The information types listed under question 1.1 are retained. They are as follows: Name, Social Security Number (SSN), Date of Birth, Personal Phone Number, Personal E-mail address, Race/Ethnicity, Gender, Integrated Control Number (ICN), UserID, Username, Mailing Address, financial account information, loan information such as Loan ID, loan payment amounts, liquid assets value, FICO, household income, disability percentage from VA, Purple Heart recipient, Veteran's tours of duty including character of discharge.

3.2 How long is information retained?

*In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. **The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.** If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

The information is retained indefinitely.

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?

Retention schedule has been approved by the National Archives and Records Administration (NARA). The Records Control Schedule is VB-1 Part 1, Section, XIII, Veterans Benefits Administration Records Management, Records Control Schedule VB-1 Part 1, Section VII. VHB will follow the guidelines for retaining data as identified in the Loan Guaranty SORN 55VA26. Computerized electronic records in VA information systems are kept indefinitely. Records in individualized case folder concerning Native American Direct and Refunded/Acquired Loans are retained at the VA servicing facility until the contract expires then are transferred to the new vendor. Active direct loan case folders are retained at the VA servicing facility until the case becomes inactive (e.g., loan is paid in full). Inactive guaranteed and direct loan folders are forwarded to private retention facility, Iron Mountain, retained for five years and then destroyed. Specially adapted housing (SAH) records are maintained either at VA Central Office (VACO) and/or the VA servicing facility.

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

VHB retains individual's veteran's file folders, claims records, and loan information accessible through VHB 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.

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.

Individual veteran's file folders, claims records, and loan information accessible through VHB 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.

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.

VHB protects PII data for testing purposes in the same manner as it protects production or operational PII data. Any use of PII for testing, such as testing new applications, is conducted within the VHB security authorization boundary and subject to the same controls as the VHB production 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: Veteran data is retained indefinitely. Individual Veteran's file folders, claim records, and loan information accessible through VHB 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. If this information is breached or accidentally released to inappropriate parties or the public, it could result in financial, personal and/or emotional harm to the individuals whose information is contained in the system.

Mitigation:

- Paper records are maintained/disposed of in accordance with the VHB Records Control Schedule.
- All personnel with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.
- VHB adheres to all information security requirements instituted by the VA Office of Information Technology (OIT).

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***
LGY Cloud Assessing	Migration of data from LGY to VHB	Veteran Name, Date of Birth (DOB), Social Security Number (SSN), Mailing address, personal contact number, personal e-mail address, Loan Information (loan ID number, loan payment amounts)	Site-to-site encrypted transmission

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: There is a risk that VHB data may be shared with unauthorized users or authorized users may share data with other unauthorized individuals.

Mitigation:

- All personnel with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.
- LGY adheres to all information security requirements instituted by the VA Office of Information Technology (OIT)
- Information is shared in accordance with VA Handbook 6500.

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	***List the purpose of information being shared /***	***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,***	***List the method of transmission and the measures in***

shared/received with	***received / transmitted with the specified program office or IT system***		***SORN routine use, etc. that permit external sharing (can be more than one)***	***place to secure data***
Pay.gov		First Name, Last Name, Date of Birth (DOB), Social Security Number (SSN), Mailing Address, Personal Contact number, Personal email address, Race/ Ethnicity, Loan Information (loan id number, loan payment amounts) Financial account information.	MOU/ISA	REST API
SAM.gov		First Name, Last Name, Date of Birth (DOB), Social Security Number (SSN), Mailing Address, Personal Contact number, Personal email address, Race/ Ethnicity, Loan Information (loan id number, loan payment amounts) Financial account information.	MOU/ISA	REST API
GNMA		Loan Information, Address	MOU/ISA	REST API
HUD		Loan Information, Address	MOU/ISA	REST API

5.2 <u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>

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

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

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk: There is a risk that LGY data may be shared with unauthorized users or authorized users may share it with other unauthorized individuals.
Mitigation: Outside agencies provide their own level of security controls such as access control. Authentication and user logs to prevent unauthorized access.

- All personnel with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.
- LGY adheres to all information security requirements instituted by the VA Office of Information Technology (OIT.)
- Information is shared in accordance with VA Handbook 6500.

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.

At the time of data collection, a Privacy Notice is given to the user by the entity that is collecting the information, as stated above VHB does not collect PII directly from Veterans.

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

A Privacy Notice is given to the user by the entity that is collecting the information, not by the VA or VHB.

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

The notice explains why the PII or SPI data is being collected and what the data will be used for within VHB. The notice also specifies the effects of providing information on a voluntary basis and that the data collected may specify "routine use". The following privacy websites are available for reference: SORNs: http://www.oprm.va.gov/privacy/systems_of_records.aspx

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.

Individuals 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.

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. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

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

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

Privacy Risk: There is a risk that the user may not understand that the data entered will go into a long-term records system or that PII data may be shared with outside agencies.

Mitigation: A privacy notice is given to the user as stated in Section 6.1 that states that the system exists in detail, along with the Privacy Act Statement of Records Notice. Section 7. Access, Redress, and Correction

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

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

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

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

The following procedures are 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 making 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 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, 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 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 details is based, and advise that the denial may be appealed in writing to the General Counsel (024), Department of Veterans Affairs, 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 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 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 thereafter, and of his or her right to seek judicial review of the decision pursuant to section 3 of the Privacy Act (5 U.S.U. 552a(g)). (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 facts 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 the statement of disagreement will be provided, and, when appropriate, copies of the statement of VA's reasons for making the amendment(s) requested will also be provided. (11) A decision by either the General Counsel or Deputy General Counsel pursuant to paragraph in which 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.

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

The system is not exempt from the access provisions of the Privacy Act.

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

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-digital lender identification number assigned by 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 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.

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. The validation that accurate information is provided is built into the loan application process as described in section 1.5.

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 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.

No alternatives are provided. The Veteran and lender work together to gather all 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 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 as described in section 1.5 (and in the migration plan in section 7.5).

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 considering 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 can 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: There is a risk the individual accidentally provides incorrect information in their correspondence with the Lender.

Mitigation: The information entered VHB is gathered by the lender during the loan application process. Additionally, during this process, the information is validated through the submission of documentary evidence provided by the Veteran, Lender, and VA Loan Guaranty.

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?

User access is requested via the "new user request" form within Salesforce (https://va.my.salesforce-sites.com/helpdesk/VA_Help_Desk_New_User_405). The form includes a drop-down field "Application Requested" (i.e. VALERI, Veteran Home Benefits). Based on the application requested, once the form is submitted, the application approvers receive an email informing them of the request. The approver logs into Salesforce, reviews the request, and approves/denies the request. If approved, a case will be submitted to the DTC help desk to create the user and provision the access. With this process, there are only 2 approvers (the primary and backup approvers). DTC is in the process of moving the new user request process to ServiceNow. While the exact details of this process are not yet solidified, it is expected that the user will submit requests via the ServiceNow yourIT Portal. The request will be assigned to a project/application "assignment group" for review and approval.

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?

VHB does not provide access to the system to users from other agencies.

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.

Account permissions are managed in the VHB Salesforce front end application utilizing Role-Based Access Control model, whereby user access to the system is determined by the role the user is assigned when the account is provisioned.

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.
Contactors who have access to the system and PII have a signed NDA on file during the on-boarding process. Some regular users of VHB are authorized VA and contract employees. There are contract system administration personnel within the Salesforce GovCloud Plus Enterprise (SFGCP-E) who maintain the server hardware and software but are not privileged users of the VHB system itself. Contracts are reviewed annually by the VHB application's Program Manager, Information System Owner, Information Owner, Contract Officer, Privacy Officer, and the Contracting Officer's Technical Representative.

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

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

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 or information. Please describe how individuals who have access to PII are trained to handle it appropriately.
This question is related to privacy control AR-5, Privacy Awareness and Training.

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

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

Yes

8.4a If Yes, provide:

1. *The Security Plan Status:* Completed
2. *The System Security Plan Status Date:* 10-APR-2024
3. *The Authorization Status:* Approved
4. *The Authorization Date:* 03-May-2024
5. *The Authorization Termination Date:* 03-May-2026
6. *The Risk Review Completion Date:* 25-Apr-2024
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* High

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

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***

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 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, VHB utilizes PaaS and SaaS hosted by Salesforce GovCloud Plus – Enterprise (SFGCP-E) for the Front-End application and back-end systems hosted in VAEC AWS GOVCLOUD HIGH to support the SFGCP-E front-end application.

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.*

Yes, Service Provider: "Salesforce Subscription Licenses, Maintenance and Support", Contract Number: NNG15SD27B, Order Number: 36C10B9F0460. CLIN SWF-5700.

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.

No, CSP will not collect ancillary data, and VA has ownership over all data.

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.

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).

VHB is not utilizing Robotics Process Automation (RPA).

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: 2024.06.30 21:20:19 -04'00'

Privacy Officer, Chiquita Dixson

PATRICK STANFORD

Digitally signed by PATRICK STANFORD
Date: 2024.06.28 11:22:58 -05'00'

Information System Security Officer, Patrick Stanford

TERRANCE WILSON

Digitally signed by TERRANCE WILSON
Date: 2024.06.28 09:17:23 -04'00'

Information System Owner, Terrance Wilson

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy; a Privacy Act notice on forms; screen shot of a website collection privacy notice).

PRIVACY ACT NOTICE-VA will not disclose information collected on this form to any source other than what has been authorized under the Privacy Act of 1974 or Title 38, Code of Federal Regulations 1.576 for routine uses (for example: the authorized release of information to Congress when requested for statistical purposes) identified in the VA system of records, 55VA36, Loan Guaranty Home, Condominium and Manufactured Home Loan Applicant Records, Specialty Adapted Housing Applicant Records, and Vendee Loan Applicant Records-VA, and published in the Federal Register. Your obligation to respond is required in order to determine the qualifications for a loan. Your obligation to respond is required to obtain or retain benefits. Giving us your SSN account information is voluntary. Refusal to provide your SSN by itself will not result in the denial of benefits. VA will not deny an individual benefits for refusing to provide his or her SSN unless the disclosure of the SSN is required by a Federal Statute of law in effect prior to January 1, 1975, and still in effect.

HELPFUL LINKS:

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

VA Privacy Service Privacy Hub:
https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):
VHA Notice of Privacy Practices
VHA Handbook 1605.04: Notice of Privacy Practices