Privacy Impact Assessment for the VA IT System called:

Appraisal Management Services

VA Loan Guaranty Service

Veterans Benefits Administration

Date PIA submitted for review:

01/13/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Chiquita Dixson	Chiquita.Dixson@va.gov	202-632-8923
Information System Security Officer (ISSO)	Robert Gaylor	Robert.Gaylor@va.gov	720-874-1030
Information System Owner	Randy Cope	Randy.Cope@va.gov	202-632-8788

Abstract

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

Appraisal Management Services (AMS) is one of sub systems that comprises the Loan Guaranty (LGY) Major Application. AMS is a managed system by The Veros Appraisal Management Services (AMS) and Other Related Services (ORS) is a refactoring and modernization of an existing appraisal management services program, which conceptualizes a phased approach to accomplish a fully integrated, appraisal management solution from the initial appraisal request and assignment through the issuance of a VA guaranty.

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?*

VA Benefits and Memorials (BAM)-Loan Guaranty (LGY)VA BAM LGY to increase Veteran home ownership. Veros AMS shall provide the Construction and Valuation (C&V) staff, lenders, servicers, and appraisers services that improve risk management, timeliness, and performance, as well as the credibility and quality of valuation functions. Veros AMS will improve services to Veterans, oversight capabilities to ensure accuracy of appraisal reports as VA appraisals are performed to protect the interests of the program and all program participants**.**to support the procurement of VA Automated

Appraisal Management Services (AMS) to further enhance the appraisal review process, thereby improving the oversight functions of C&V.

AMS tracks the appraisal order that is created in the VA WebLGY application and facilitates the scheduling of the onsite inspection by the appraiser. AMS receives the appraisal report uploaded by the appraiser into LGYHU/WebLGY and performs an electronic scoring based on VA requirements and using data collected from VA appraisals and other sources. AMS provides the data and results of the scoring and electronic screening review, and collects the data from the appraisal reports for use by VA. The ORS system allows the C&V staff to order additional appraisal collateral products to aid them in their review process.

AMS application is hosted within Veros data center and integrated with WebLGY through system-to-system API calls through the api.va.gov API gateway and single sign on through the AccessVA identity provider. The expected number of individuals whose information is stored in the system is approximately 100,000. Veros AMS shall provide the Construction and Valuation (C&V) staff, lenders, servicers, and appraisers services that improve risk management, timeliness, and performance, as well as the credibility and quality of valuation functions. Veros AMS will also store appraisal records.

Information Type Transmitted: Information to be transmitted will include VA owned Sensitive Information and Personally Identifying Information (PII) sent to Veros AMS.

Data Flow Description: The data to be transferred from LGY consists of property appraisals (subject property, borrower and appraiser name, address, phone number, email address, images of the property, property descriptive information, and loan ID number).

The authority for this interconnection is based on: Loan Guaranty Service Federal Information Security Modernization Act of 2014 (FISMA 2014)

- VA Directive 6500, VA Directive 6500: VA Cybersecurity Program, *and Handbook 6500, Risk Management Framework for VA Information Systems: Tier 3 – VA Information Security Program*
- 38 United States Code (U.S.C.) §§ 5721-5728, Veteran's Benefits, Information Security
- Office of Management and Budget (OMB) Circular A-130, Appendix III, Security of Federal Automated Information Systems
- 18 U.S.C. 641 Criminal Code: Public Money, Property or Records
- 18 U.S.C. 1905 Criminal Code: Disclosure of Confidential Information

The authority for Loan Guaranty Service to share data for the purpose outlined under this Agreement with the recipient is as follows: Loan Guaranty Service

- Privacy Act of 1974, 5 U.S.C. § 552a, as amended
- The disclosure authority for any Privacy Act protected information is: 5 U.S.C. § 522a (b)(3); Routine Use #20 of VA System of Records 55VA26.
- VA Claims Confidentiality Statute, 38 U.S.C § 5701

There will not be any changes to business processes as a result of this PIA. The completion of this PIA will not cause any change to technology. The SORN will require amendment. The systems use Amazon Web Services and has FedRAMP Authorization which complies with VA Handbook 6517. LGY has a contract with AWS, and Veros which establishes who has ownership rights over the data in the systems.

- Veros AMS will retain all records, data, metadata, and data/database architecture/configuration pertaining to each property and appraisal, and each transaction. Records and related documentation, as well as data and database architecture/configuration are VA's property and, upon termination of this contract, the contractor shall deliver to VA or its designee, those, as well as all nonstandard requirements that help VA and the new contractor understand the operational environment at the current contractor's expense.

The owners of LGY and Veros AMS agree to designate and provide contact information for the technical lead(s) for their respective system, and to facilitate direct contact between technical leads to support the management and operation of the interconnection. To safeguard the confidentiality, integrity, and availability of the connected systems and the data stored, processed, and transmitted, the parties agree to provide notice of specific events immediately.

- Home Information such as found on multiple listing services (MLS) is public.
- Veterans' financial information is PII and not public.
- Loan information is not public.
- Any relative information such as Veteran financial and MLS is private information because it exposes the Veteran Status.

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

- Appraiser VA ID
- Loan Identification Number
- Appraiser Work Email
- Appraiser Phone Number
- Appraiser Work Address
- Property Address

PII Mapping of Components

N/A

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
N/A					

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

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

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

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

Appraisal information is received by VA approved appraisers. The VA Appraiser or internal VA Fee Panel Appraiser will upload a Mortgage Industry Standards Maintenance Organization (MISMO) XML appraisal file to Loan Guaranty Service (LGY) WebLGY that will be transmitted via an application programing interface (API) service to the Veros AMS domain.

LGY obtains Personal Contact information, property data and Rating Diagnostics from the applicant and from other sources such as Department of Veterans Affairs (VA) files, VA/Department of Defense (DoD) Identity Repository (VADIR). Other data such as loan information is gathered for eligibility requirements.

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.

AMS does not collect information directly from individuals. The PII data elements are captured in the submission an appraisal report and various home loan documents. Appraisers provide and collect this information from the borrower of the VA Loan. Personal information is collected from the applicant or from end users on the veteran's behalf. Service information is extracted from VA files, VADIR 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), VADIR, eBenefits, Financial Management System (FMS), LGY partners such as Lenders, Services and Appraisers and the Benefits Identification and Locator System (BIRLS).

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.

AMS system shall track the appraisal order from notification to acceptance by VA. The AMS system receives the appraisal report uploaded by the appraiser and provides a validation process to ensure that the report matches the assignment. AMS system will track appraisal assignment and review timeliness from initial order through the issuance of the Notice of Value (NOV). The AMS then performs an electronic screening review function and scoring based on VA requirements and using data collected from VA appraisals and other sources. The AMS provides the data and results of the scoring and electronic screening review and collects the data from the appraisal reports for use by VA.

AMS will also provide a dashboard presenting the following information will be available to include but are not limited to:
- Appraisal workload volume and trending information
- Appraisal assignments with no appraiser assigned
- Appraisals completed timely and untimely – in conjunction with tracking application described in 4.5A (Three (3) key points – appointment set, site inspection completed, appraisal uploaded)

- Overdue and pending appraisal assignments
- Appraiser scorecards by state, county and appraiser with accuracy, timeliness, and workload data
- Appraiser license status summary dashboards

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. 17VA26/78 FR 71727(Contains Exemptions)
EXECUTIVE ORDER 9397 NUMBERING SYSTEM FOR FEDERAL ACCOUNTS RELATING TO INDIVIDUAL PERSONS

Applicant Records-VA 55VA26 by the Privacy Act of 1974, 5 U.S.C. 552a(E) (4 6, 5 U.S.C. 552a(R)and
OMB 59 FR 37906, 3791618, July 25, 1994.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:
Privacy Risk: Sensitive Personal Information including personal contact information and benefit information may be released to unauthorized individuals.

Mitigation: AMS adheres to 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 annually. 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.
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 annually.

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.
AMS Users sign into the application using VA Single Sign On via Identity and Access Management (IAM)

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 information contained in the records may include identifying information (e.g., name, address, phone number, email address, Loan Identification Number (LIN) number, or file number. Name, LIN number and/or file number are used to identify and track individual(s) in VA systems. The address is needed so that VA can send correspondence to Veterans.

AMS is a commercial off- the-shelf (COTS) product. AMS will provide information pertaining to a VA Loan Guaranty appraisal

- Deliver a high-quality experience for all stakeholders, including Veterans, lenders, and servicers who are partnering with the VA to serve them, through timely appraisal reports.
- Provide tools for conducting strong oversight to ensure accuracy of appraisal reports as VA appraisals are performed to protect the interests of the program and all program participants.
- Ensure that VA's appraisal review staff and lenders' and servicers' Staff Appraisal Reviewers (SARs) have the latest appraisal review tools and resources available in the industry in order to best serve Veterans.
- Provide innovative technology to ensure that VA is exceeding appraisal industry benchmarks. Quality appraisal services are essential in supporting VA's commitment that VA guaranteed home loans are the product of choice for Veterans.

- Provide a AMS to enhance the appraisal services provided to Veterans through VA's home loan guaranty program. VA is the leading voice in housing for our Veterans. Appraisals are critical in maximizing the opportunities for Veterans and Servicemembers to obtain and retain homes.
- Provide data, data reporting, and data analytic capabilities that support VA's objective of making data-driven policy and program decisions.

Information used in the system:

- **Name**: Used to identify the Veteran or primary subject(s) during appointments and in other forms of communication
- **Mailing Address**: Used for communication, billing purposes and calculate travel pay
- **Zip Code**: Used for communication, billing purposes, and to calculate travel pay
- **Phone Number(s):** Used for communication, confirmation of appointments and conduct Telehealth appointments
- **Email Address**: used for communication.
- **Loan Identification Number (LIN) –** number which uniquely identified a particular home loan.
- **Appraiser VA ID:** number which uniquely identifies an assigned VA appraiser.

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

AMS shall provide a phased approach to accomplish a fully integrated, appraisal management solution from the initial request and assignment through the issuance of a VA Notice of Value (NOV).

This phased approach will require: ·

- Interfaces for workflow connections to the Veros platform and WebLGY
- Enhancements to the current WebLGY to accommodate the new AMS and its features with single sign-on capability ·
- IT resources to test and ensure full compliance and functionality of the new AMS across all phases of the appraisal process to include system enhancements as needed ·
- Storage capacity for all appraisal processing data such as (appraisal reports, appraisal scoring reports (VeroSCORE) automated valuation models (VeroVALUE), etc.)

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?

Electronic responses inbound/outbound via Application Programming Interface (API) service and encrypted rest.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? AMS is not collecting stakeholder's Social Security Numbers.

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

Through the use of personal identity verification (PIV) card only access and 2-factor authentication.

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

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u> 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. <u>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.</u>

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

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

<u>Principle of Use Limitation:</u> 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.

All users must register to access the LGY Web portal. Internal users are validated against the Windows Active Directory user database, while external users are validated against the local Oracle Database. The data requests are delivered through a Secure Socket Layer (SSL) connection.
All internal employees 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 annually.
Disciplinary actions, depending on the severity of the offense, include counseling, loss of access, suspension and possibly termination.
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. The user ID is stored in both VA and the AMS. Both VA and Veros are responsible for safeguarding PII information. Both VA and Veros log and track user access to the systems. Logs are reviewed on a regular basis and any discrepancies are reported.
External users are vetted through their lender/servicer organization. An administrator within the organization authorizes the initial user registration and then validates their continued access every 90 days.
The official system of records notice (SORN) number is: 55VA26 and can be found online at: https://www.oprm.va.gov/privacy/systems_of_records.aspx

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

AMS stores the primary subject's personal information, property information and loan information. Data types include:

- Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc.)
- Loan Information
- Appraiser VA ID
- Mailing Address & Zip Code
- Phone Number(s)
- Email Address

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.

Records in individualized case folder concerning active VA guaranteed or insured loans are retained at the VA servicing facility for up to three years and forwarded to the Federal Archives and Records Center (FARC) where they are retained up to thirty-three years and then destroyed. Active direct loan case folders are retained at the VA servicing facility until the case becomes inactive, e.g., existing loan balance is paid in full. Inactive guaranteed and direct loan folders are forwarded to the FARC annually, retained for five years and then destroyed. Vendee loan records being maintained in case folders are kept at the VA servicing facility until five years after the case becomes inactive and are then destroyed. Specially adapted housing (SAH) records are maintained either at VA Central Office (VACO) and/or the VA servicing facility. Once SAH records are closed, SAH records at VACO are maintained for one year and then sent to the FARC where they are retained for thirty years and then destroyed. Closed SAH records maintained at regional offices are maintained for ten years and then destroyed. Generally, automated records (e.g., computer lists, discs, and microfiche) are maintained for up to five years and then destroyed. Destruction of records is accomplished by shredding, burning, and/or erasure. File information for CAIVRS is provided to HUD by VA on magnetic tape. After information from the tape has been read into the computer the tape is returned to VA for updating. HUD does not keep separate copies of the tape.

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.

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). 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. (https://www.benefits.va.gov/WARMS/docs/regs/RCS_I.doc).
Destroy records by shredding when suspended or obsolete.

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

VA follows the following procedures.
• Individual veteran's file folders, claims records, and loan information accessible through LGY 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 5,10,30 or 35 years based on the type of record., Records which exceed retention timeframes are thereafter destroyed at the direction of the Archivist of the United States.
Veros process is as follows:
• Retain all records, data, metadata, and data/database architecture/configuration pertaining to each property and appraisal, and each transaction. Records and related documentation, as well as data and database architecture/configuration are VA's property and, upon termination of this contract, the contractor shall deliver to VA or its designee, those, as well as all nonstandard requirements that help VA and the new contractor understand the operational environment at the current contractor's expense. This transitional period shall take place no later than 60 days prior to termination. To ensure a smooth transition out and continuity of services to VA and its customers, the contractor shall cooperate in good faith to provide information and AMS/ORS activities to the new contractor. The contractor will not continue to receive new AMS/ORS requests upon expiration of their task order but shall follow an orderly approach to transfer any necessary information to the new contractor. Records shall be provided to VA in a mutually agreeable, readable, and modifiable form compatible with VA's systems and architecture.

Records shall be kept for the life of the contract and any exercised Optional Periods, plus two (2) years.

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

Not applicable

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

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

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

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

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

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

Follow the format below:
Privacy Risk: Veteran’s data is retained indefinitely. Individual veteran's file folders, claims records, and loan information accessible through AMS are retained at the Veros data center. If this information was breached or accidentally released to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to the individual whose information is contained in the system.
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. AMS adheres to all information security requirements instituted by the VA Office of Information Technology (OIT).
Individual veteran's file folders, claims records, and loan information accessible through LGY 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 5,10,30 or 35 years based on the type of record. Records are thereafter destroyed at the direction of the Archivist of the United States.

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 data element types such as PII/PHI that are shared/received with the Program Office or IT system***	***Describe the method of transmittal***
WebLGY	WebLGY interface is used to receive and send VA appraisal report information. The appraisal report uploaded by the appraiser into WebLGY and performs an electronic scoring based on VA requirements and using data collected from VA appraisals and other sources. records, and process benefits as applicable.	Lender, Appraisers Borrower full name, phone numbers, property address, business address, email address, case number, file number	Data is transmitted securely: electronic responses inbound/outbound via Application Programming Interface (API) service

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

Follow the format below:

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

Mitigation: The VA provides Windows and Oracle access controls along with the following security controls: Audit and Accountability, Awareness Training, Security Assessment and Authorization, Incident Response, Personnel Security, and Identification and Authentication.

- 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	*List the purpose of information being*	*List the specific PII/PHI data elements that are*	*List the legal*	*List the method of transmission*

or IT System information is shared/received with	***shared / received / transmitted with the specified program office or IT system***	***processed (shared/received/transmitted) with the Program or IT system***	***authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***and the measures in place to secure data***
AMS	1.AMS will facilitate the scheduling of the onsite inspection by the appraiser. 2.AMS will receive the appraisal report uploaded by the appraiser into VA LGYHUB site and performs an electronic scoring based on VA requirements and using data collected from VA appraisals and other sources. 3.AMS will also provide the data and results of the scoring and electronic screening review, and collects the data from the appraisal reports for use by VA.	• Veteran First Name • Veteran Last Name • Property Address • Loan Identification Number (LIN) • Appraiser First Name • Appraiser Last Name • Appraiser Work email address • Appraiser Work Phone Number • Appraiser VA ID • Property Owner First Name • Property Owner Last Name	ISA/ MOU	Electronic responses inbound/outbound via Application Site to Site (S2S) through API service. Data is transmitted via REST API.

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: There is a risk that AMS data may be shared with unauthorized users or authorized users may share it with other unauthorized individuals. Additionally, misspelling the veteran's name could result in the wrong data to be displayed.

Mitigation: Outside agencies provide their own level of security controls such as access control, authentication, and user logs in order 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 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.

The following privacy websites are available for reference:

SORNs:

1) VA SORN 55VA26: Loan Guaranty Home, Condominium and Manufactured Home Loan Applicants Records, Specially Adapted Housing Applicant Records and Vendee Loan Applicant RecordsVA

2) 17VA26): Loan Guaranty Fee Personnel and Program Participant Records-VA

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 appraiser; however, without providing the information the appraiser cannot originate an order for an appraisal.

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 and/or appraiser 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: 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 and a System 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?

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.

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 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 5U.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), 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 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)).

(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.

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.
Veterans can request to review their information for accuracy by contacting the VA Regional Loan Center Responsible for their area

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 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 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 mitigation 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.

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

<u>Principle of Individual Participation:</u> 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?

<u>Principle of Individual Participation:</u> 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: There is a risk the individual accidentally provides incorrect information in their correspondence with the Lender.

Mitigation: The information entered AMS 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.
VA Regional Loan Center Staff review a subset of eligibility requests and loan guaranty records that do not obtain automatic approval. Additionally, a subset of records is reviewed for quality assurance purposes. All Specially Adapted Housing (SAH) application data is strictly reviewed by SAH agents. These audits include a review of the original application submitted by the Veteran, correspondence logs, relevant documentary evidence, and information in existing VA systems (WebLGY, SHARE, etc.).

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. Appraiser, and other services from the appraisal community are reviewed and approved by the VA prior to onboarding to use the AMS Regular users of LGY are authorized VA and contract employees. There are contract system administration personnel within the VA Enterprise Cloud (VAEC) who maintain the server hardware and software but are not privileged users of the LGY system itself.

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 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.

Veros employees' employment agreements contain NDA provisions that apply to confidential VA information employees are exposed to as part of the AMS contract, as does Veros' contract with the VA, but individual Veros employees do not sign an NDA directly with the VA.

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

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

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB (for AITC 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 re- affirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. All VA employees must complete annual Privacy and Security training.

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

If Yes, provide:

1. *The date the Authority to Operate (ATO) was granted,*
2. *Whether it was a full ATO*
3. *The amount of time the ATO was granted for, and*
4. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

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

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

The AMS program was granted a renewal ATO for 365 days on March 12, 2021. AMS is a moderate security categorization system.

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).

Yes, *Veros Real Estate Solutions (MSaaS).* All functions and support provided by the Contractor is done remotely from their cloud environment. The agreement that's in place between VA and CSP is documented in *Veros VA System LGY MOU ISA - Fully signed and Executed Annual Review_06142021.pdfThis 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.

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.

The Veros Appraisal Management Services contract number: 36C10X19C0033

Adequate security controls for collecting, processing, transmitting, and storing of Personally Identifiable Information (PII), as determined by the VA Privacy Service, must be in place, tested, and approved by VA prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of VA. These security controls are to be assessed and stated within the PIA and if these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection of PII.

Veros Real Estate Solutions (VEROS) implements the following security measures and controls: To be completed by Veros Real Estate Solutions (VEROS)

- Patch management policy - Operating systems are periodically updated with new releases or patches from vendors. Changes to the operating system must be tested in a testing environment and reviewed to ensure that there are no adverse impacts on security. Operating system change control procedures include:
    - Vendor recommended patches must be analyzed for applicability in the Veros environment and tested before applying them to production systems
    - Implementation of operating system changes including rollback planning and review of security controls.
- Malware prevention / Virus Scanning policy - Virus-checking systems approved by Information Security must be in place on all computers with operating systems susceptible to viruses, on all firewalls with external network connections, and on all electronic mail servers. All files coming from external sources must be checked before execution or usage. If encryption or data compression has been used, these processes must be reversed before the virus-checking process takes place. Users must not turn off or disable virus-checking systems.
- Audit policy – Veros's audit policy provides independent and objective assurance as well as advisory services designed to add value and improve Veros' control environment which is accomplished through a systematic and disciplined approach to evaluate, monitor, and improve the effectiveness of internal controls, risk management support, and compliance monitoring.
- Incident response / security breach notification policy - Incident Response Plan (IRP) provides mitigation strategies and responses to intentional or inadvertent information security events affecting the confidentiality, integrity, and availability of information, automated information systems and networks. It also includes procedures for organizational actions in response to computer security incidents. The person who discovers the Incident will notify

the Sr. Vice President of Technology. If the person discovering the incident is not a member of the IT department or affected department, they will email the Veros helpdesk who will notify the Sr. Vice President of Technology. If an IT staff member receives a call (or discovered the Incident and/or Event) they will log the Incident and/or Event in the issues tracking system and refer to their contact list for both management personnel and incident response team members to be contacted. The staff member will contact the Incident response manager using both email and phone messages while being sure other appropriate and backup personnel and designated managers are contacted.

- User certification, identification, and authentication policy - The logon process for network-connected Veros computer systems must simply ask the user to log on, providing prompts as needed. Specific information about the organization managing the computer, the computer operating system, the network configuration, or other internal matters must not be provided until a user has successfully provided both a valid user ID and a valid password.

- Password policy - Users must choose difficult-to-guess passwords. Fixed passwords must not be found in the dictionary and must not be a reflection of the user's personal life. All fixed passwords must be at least 8 characters, and this minimum length must be enforced automatically where systems support it. Users must choose fixed passwords that include both alphabetic and numeric characters and users must change their passwords every ninety (90) days.

- Account Management policy – Veros accounts are created upon management approval or request from Human resources for new hires. Additional access requests are tracked in the ticketing system and approved by management. Accounts are audited every ninety (90) days. Upon employee termination, account is terminated within twenty-four (24) hours.

- Physical and environmental security policy - Access to all Veros facilities is secured by proper access control measures. Entry and exits to restricted areas are monitored and recorded 24/7 by digital means and stored for a period of at least 30 days. Recording and storage is verified regularly.

- Firewall, IDS, and encryption policy - An external router receives incoming traffic from the Internet and other external data sources. Incoming traffic is routed through redundant IPS/firewalls, which restrict unauthorized access to or from the internal network. These measures protect against typical network-based attacks. There is an ability to enforce specific rules and policies on outgoing/incoming services and applications. The IPS/firewall appliances have the ability to detect common Internet attacks, generate alert notifications and initiate pre-established response measures. Only the necessary ports on the firewall are enabled for use. The IPS and firewall system are updated continually to minimize the potential for network security vulnerabilities to be exploited.

  Encryption of information in transit must be achieved through commercially available products approved by Information Security. Whenever encryption is used, workers must not delete the sole readable version of the information unless they have demonstrated that the decryption process is able to reestablish a readable version of the information. Encryption keys used for Veros information are always classified as Confidential or Secret information.

Access to such keys must be limited only to those who have a need to know. Unless the approval of the Information Services manager is obtained, encryption keys must not be revealed to consultants, contractors, temporaries, or other third parties. Encryption keys always must be encrypted when sent over a network. TLS encryption is available for all Website access.

FIPS policy is enforced in Active Directory via GPO security policy for the application servers. FIPS mode is enabled on Identity Access Management (IAM) servers. The Veros AMS solutions also utilize an Oracle database and FIPS is configured and implemented via database initialization parameters. Network attached storage (NAS) utilized self-encrypting drives and Storage Area Network (SAN) is FIPS 140-2 compliant and keys are automatically rotated daily (every 24 hours) or whenever any hardware change is made to the system.

- Contingency Plans - Department managers who define the backup schedule are also responsible for preparing and periodically updating user department contingency plans to restore service for all production applications, despite whether internal network services are required for the support of these applications. The Information Technology Department is responsible for preparing and periodically updating network service contingency plans.

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.

Not applicable.

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.

Both parties are responsible for auditing application processes and user activities involving the interconnection with sufficient granularity to allow successful investigation and possible prosecution of wrongdoers. Activities that will be recorded include event type, date and time of event, user identification, workstation identification, success or failure of access attempts, and security actions taken by system administrators or security officers. Audit logs will be retained for a minimum of one (1) year or as documented in the National Archives and Records Administration (NARA) retention periods, or whichever is greater. Audit logs which describe a security breach must be maintained for six (6) years. Those responsible for maintaining audit logs must ensure that audit logs are successfully stored for the required duration.

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.

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**

ID	Privacy Controls
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 126558

Digitally signed by Chiquita Dixson 126558
Date: 2022.03.15 08:30:02 -04'00'

Privacy Officer, Chiquita Dixson

DN: dc=gov, dc=va, o=internal, ou=people, 0.9.2342.19200300.100.1.1=robert.gaylor@va.gov, cn=Robert S. Gaylor 1130634
Date: 2022.03.17 06:36:53 -06'00'

Information System Security Officer, Robert Gaylor

RANDY E. COPE 1013890

Digitally signed by RANDY E. COPE 1013890
Date: 2022.03.18 07:43:52 -04'00'

Information System Owner, Randy Cope

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).

http://www.oprm.va.gov/privacy/systems_of_records.aspx