Privacy Impact Assessment for the VA IT System called:

Veterans Legacy Memorial Assessing (VLM)

National Cemetery Administration (NCA)

Office of Information and Technology (OIT)

eMASS ID #1026

Date PIA submitted for review:

02/20/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Cindy Merritt	Cindy.Merritt@va.gov	321-200-7477
Information System Security Officer (ISSO)	Ronald Cox	Ronald.Cox@va.gov	414-902-5613
Information System Owner	Erin Fincham	Erin.Fincham@va.gov	202-815-9381

Abstract

The abstract provides the simplest explanation for "what does the system do?".

VLM is an online memorial that honors nearly 10 million Veterans interred in VA National Cemeteries, VA grant-funded cemeteries, DoD-managed cemeteries (including Arlington National Cemetery); U.S. Park Service National Cemeteries, and thousands of private cemeteries where Veterans have received a VA-provided gravesite marker since 1996. The deceased Veterans' info is only displayed when searched by name. The list of information displayed is critical in maintaining Veterans' legacies. All Veteran data published on VLM is no longer PII and is public record. The Living Veteran feature provides a living Veteran with the ability to drive how they will be remembered.

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?

Veterans Legacy Memorial (VLM) is owned through a partnership between the National Cemetery Association and the Office of Information and Technology.

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

VLM is a public-facing website designed to honor deceased Veterans' legacies. Nearly 10 million records are available to the public to view the deceased Veteran's profile in VLM. The deceased Veterans' info is only displayed when searched by name. The list of information displayed is critical in maintaining Veterans' legacies. All Veteran data publicly viewable on VLM is no longer PII and is public record.

C. Who is the owner or control of the IT system or project?

Veterans Legacy Memorial is VA owned and VA operated.

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?

VLM is an online memorial that honors nearly 10 million Veterans interred in VA National Cemeteries, VA grant-funded cemeteries, DoD-managed cemeteries (including Arlington National Cemetery); U.S. Park Service National Cemeteries, and thousands of private cemeteries where Veterans have received a VA-provided gravesite marker since 1996. VLM also will host approximately 200,000 Living Veteran pages that are not viewable to the public and are accessible only to the Living Veteran themselves.

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

Veterans Legacy Memorials (VLM) is part of the Memorials Benefits Appeals and Memorial (BAM) portfolio. National Cemetery Administration partners with OIT and owns VLM. VLM is a public facing website designed to honor deceased Veterans' legacies. Nearly 10 million records are accessible by the public to view the deceased Veteran's profile in VLM. The deceased Veteran's info is only displayed when searched by name. All Veteran data published on VLM is no longer PII and is public record. VLM also will host approximately 200,000 Living Veteran pages that are not viewable to the public and are accessible only to the Living Veteran themselves.

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

Burial Operation Support System (BOSS) database, Enterprise Interment Services System (EISS), and Automated Monument Application System (AMAS) for deceased Veterans public information (Name; Rank; DOB; DOD; Branch Of Service; Cemetery Name, Cemetery Address, Phone Number, and URL; Medals/War Period; Emblem Of Belief; KIA/MIA/POW designation) and Eligibility Office Automation System (EOAS) for living Veterans' data (Name; Rank; DOB; Branch Of Service; Medals/War Period;). Users can log in using PIV or ID.me. Users who do not want to log in using PIV or ID.me can submit content if they provide their name and e-mail address.

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?

There is no sharing conducted by VLM to any other IT system. VLM is hosted at one location VA Enterprise Cloud (VAEC) AWS (Amazon Web Service).

3. Legal Authority and SORN

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

VLM has the legal authority to use the following: 5 U.S.C. § 552a, Freedom of Information Act of 1996, As Amended By Public Law No. 104---231, 110 Stat. 3048 • 5 U.S.C. § 552a, Privacy Act of 1974, As Amended • Privacy Act of 1974; U.S. Code title 5 USC section 301 title 38 section 1705, 1717, 2306-2308 &Title 38 US Code section 7301 (a) and Executive Order 9397 • The legal authority is 38 U.S.C 7681-7683 • OMB Memo Circular A~-130, Management of Federal Information Resource, 1996 • OMB Memo M~-99—18, Privacy Policies on Federal Web Sites • OMB Memo M---03---22, OMB Guidance for Implementing the Privacy Provisions • OMB Memo M---07---16, Safeguarding Against and Responding to the Breach of PII • SORN 48VA40B, SORN 42VA41 • Authority for Maintenance of the system -Public Law 93-43 • Title 38, United States Code, § 501

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 updated and does not require amendment or revision and approval. The SORN does not discuss cloud usage or storage.

4. System Changes

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

This PIA will not result in any circumstances that require changes to business processes.

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

This PIA will not result in technology changes.

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: Veteran Names, Veteran Date of Birth, Veteran Branch of Service, Veteran Ran, and Veteran Medals/War Periods.

PII Mapping of Components (Servers/Database)

Veterans Legacy Memorial consists of 1 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 Veterans Legacy Memorial 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
MySQL (RDS)	Yes	Yes	Name; Rank; DOB; Branch of Service; Medals/War Period	To support the living veteran feature	TLS MySQL Connection

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?

Guest users who would like to submit content without logging in using PIV or ID.me account must provide name and e-mail address.

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.

Guest users provide their name and e-mail address directly. VLM does not request data from other sources.

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

Veterans Legacy Memorial does not create any new information from the information collected.

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?

Users who would like to submit content must provide their name and e-mail address. Any name and e-mail address voluntarily submitted will not be ported outside of the VLM environment or used for any other purposes other than previously described.

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?

Veterans Legacy Memorial does not collect information on forms.

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

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

Veterans Legacy Memorial does not review user submitted names and email addresses for accuracy. NCA does not review user-submitted content on the site for accuracy, but content is reviewed to ensure it conforms to the VLM user policy, which excludes content that contains: Advertisements; Dishonors Veterans; Contains Personal Identifiable Information (PII); Political; Violates Intellectual Property Law; Defamatory; Obscene; Threatening; Incites Illegal Activity.

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?

Veterans Legacy Memorial does not check for accuracy through a commercial aggregator of information.

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

U.S.C. § 552a, Freedom of Information Act of 1996, As Amended By Public Law No. 104---231, 110 Stat. 3048 • 5 U.S.C. § 552a, Privacy Act of 1974, As Amended • Privacy Act of 1974; U.S. Code title 5 USC section 301 title 38 section 1705, 1717, 2306-2308 &Title 38 US Code section 7301 (a) and Executive Order 9397 • The legal authority is 38 U.S.C 7681-7683 • OMB Memo Circular A~-130, Management of Federal Information Resource, 1996 • OMB Memo M~-99—18, Privacy Policies on Federal Web Sites • OMB Memo M---03---22, OMB Guidance for Implementing the Privacy Provisions • OMB Memo M---07---16, Safeguarding Against and Responding to the Breach of PII • SORN 48VA40B • Authority for Maintenance of the system -Public Law 93-43 • Title 38, United States Code, § 501.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: There is a risk that information may be accessed by unauthorized individuals.

Mitigation: The interface is integrated with Identity Access Management (IAM) to ensure proper authorization of user credentials prior to accessing the data store ensures proper access is granted. VLM interface utilizes a log file to capture all transactions with the interface. Incident

response is documented and managed within the portal. The security controls are designed and developed in both the software and network topology to prevent the access and disclosure of information. We use access controls, audit logs, incident response, risk management, etc.

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
Guest user name	No internal use	To send emails for submission acceptance, submission rejections, and submission flags.
Guest user email	No internal use	To send emails for submission acceptance, submission rejections, and submission flags.
Veteran Name	To support Living Veteran feature	No external use
Veteran Date of Birth	To support Living Veteran feature	No external use
Veteran Branch of Service	To support Living Veteran feature	No external use
Veteran Rank	To support Living Veteran feature	No external use
Veteran Medals/War Period	To support Living Veteran feature	No external use

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?

VLM is a one-way information system platform that displays Veteran information from Burial Operation Support System (BOSS) database, Enterprise Interment Services System

(EISS), Eligibility Office Automation System (EOAS), and Automated Monument Application System (AMAS). New records are not created, and existing records are not modified by VLM. User information is containerized and does not alter the original Veteran records - it is displayed only on the specific Veteran profile page in VLM.

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.

VLM is a one-way information system platform that displays Veteran information from Burial Operation Support System (BOSS) database, Enterprise Interment Services System (EISS), Eligibility Office Automation System (EOAS), and Automated Monument Application System (AMAS). New records are not created, and existing records are not modified by VLM. User information is containerized and does not alter the original Veteran records - it is displayed only on the specific Veteran profile page in VLM.

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?

PII is stored in a FIPS 140-2 compliant data structure and on an encrypted platform. Data manipulation is controlled by 2-factor authentication Role-Based access to the system.

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

Veterans Legacy Memorial does not collect, process, or retain Social Security Numbers.

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

Data manipulation is controlled by 2-factor authentication Role-Based access to the system. Access is controlled by management.

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

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:

<u>Principle of Transparency:</u> 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?

Data manipulation is controlled by 2-factor authentication Role-Based access to the system. Access is controlled by management.

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

Data manipulation is controlled by 2-factor authentication Role-Based access to the system. Access is controlled by management.

2.4c Does access require manager approval?

Data manipulation is controlled by 2-factor authentication Role-Based access to the system. Access is controlled by management.

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

Access to database is tracked and logged with Cloudwatch.

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

Data manipulation is controlled by 2-factor authentication Role-Based access to the system. Access is controlled by management.

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

Guest user's Name and E-mail address; Living Veterans' name, date of birth, branch of service, rank, medals/war period.

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.

VLM will utilize BOSS SORN number (48VA40B) for the coverage of guest user e-mail address. BOSS SORN 48VA40B can be found at the following URL: https://www.gpo.gov/fdsys/pkg/FR-2010-10-21/pdf/2010-26490.pdf

VLM will utilize SORN number 42VA41 for the coverage of Living Veteran data. SORN 42VA41 can be found at the following URL. https://www.govinfo.gov/content/pkg/FR-2023-09-15/pdf/2023-20046.pdf

All VLM data is kept forever, it is not deleted in accordance with the schedule approved by the Archivist of the United States, NCA Records Control Schedule, NC1–15–85–9 item 21g(1)(a).

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?

All VLM data is kept forever, it is not deleted. VLM data is kept in accordance with NC1-15-85-9. Records in this system are retained permanently in accordance with the schedule approved by the Archivist of the United States, NCA Records Control Schedule, NC1–15–85–9 item 21g(1)(a). https://www.federalregister.gov/documents/2023/05/09/2023-09838/privacy-act-of-1974-system-of-records

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

All VLM data is kept forever, it is not deleted. VLM data is kept in accordance with NC1-15-85-9. Records in this system are retained permanently in accordance with the schedule approved by the Archivist of the United States, NCA Records Control Schedule, NC1–15–85–9 item 21g(1)(a).

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.

VLM does not eliminate or transfer any information. Retention period for VLM is forever.

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.

Testing in the production system is confined to smoke testing on a fake profile, no training is conducted on this system. The purpose is allowing the public to honor and memorialize their deceased Veterans.

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: Information could be stored forever if VLM is available to the public.

Mitigation: The deceased Veterans record would be available indefinitely unless NCA approves that a specific profile page will be locked for the submission of user-provided content.

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***
Eligibility Office Automation System (EOAS)	To support the Living Veteran feature within VLM	Living Veteran name, date of birth, branch of service, rank, and medal/war period	TLS Secure Oracle

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: VLM receives Veteran data via a database query to MDW (Memorials Data Warehouse) creating a risk that PII data could be shared with an unintended VA organization, resulting in a breach of privacy and the disclosing of PII to inappropriate recipients.

Mitigation: VLM uses TLS Secure Oracle connection to transfer PII.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
None	None	None	None	None

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.

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: VLM does not share PII externally.

Mitigation: VLM does not share PII externally.

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.

VLM display terms of service and provided privacy information before users submit their e-mail address, comments, photos, and other content. SORN 48VA40B, https://www.gpo.gov/fdsys/pkg/FR-2010-10-21/pdf/2010-26490.pdf

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

Notice is provided – User Policy can be found at the following address:
https://www.cem.va.gov/VLM/userpolicy.asp

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 VLM User Policy which all users must agree to before being able to submit content, informs users how their information is being collected and used. However, users can use VLM without providing any identifying information.

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.

Guest users not wanting to log in using PIV or ID.me must provide their name and email address in order to submit content for a Veteran's profile page, but otherwise can use VLM without submitting any information. Living Veterans must have a record in EOAS (Eligibility Office Automation System) and authenticate their identity through IAM credentialling services. They do not have to provide submissions for their page if they do not want to.

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.

By submitting content to VLM, users may not place restrictions on how the VA displays or uses the information, and this is explained in the VLM User Policy which all users must agree to before being able to submit content. However, users can use VLM without providing any identifying information.

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

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:

<u>Principle of Transparency:</u> Has sufficient notice been provided to the individual?

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

This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.
Follow the format below:

Privacy Risk: There is a risk that individuals are unaware that their information is being collected or what is happening to it.

Mitigation: The notice is provided in the terms of service that must be agreed to before submitting the requested information.

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.***

VLM only displays deceased Veterans' information. Information is made public through the deployment of the VLM application. Users are only permitted to submit content to the profile and will not be able to edit deceased Veteran information. VLM does not publicly display living Veterans' data. Living Veterans are only permitted to submit content to the profile and will not be able to edit their own Veteran information.

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)?

VLM is not exempt from the access provision 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?

All deceased Veteran information displayed on VLM is public. All living Veteran information displayed on VLM is private and not public.

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.

Registered VLM users may delete or edit their submissions on the deceased Veterans page or by submitting the request to NCA; additionally, content can be flagged by any user and will be reviewed by NCA Administrators. Authenticated Living Veteran users may delete or edit their submissions on their own Living Veteran page or by submitting the request to NCA; Additionally, content can be flagged to be reviewed by NCA Administrators.

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.

In case the NCA-provided information in the VLM is inaccurate, users have the right to request an amendment of erroneous information. Individuals have the right to request a revision (or correction) to their information if they believe it is inaccurate. The individual must submit the request in writing, specify the information that should be corrected, and provide a reason to support the request for amendment. All amendment requests should be submitted to the NCA via VLM Customer Service phone (866-245-1490) or email (vlm@va.gov).

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

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

If a user believes the NCA-provided information within VLM to be inaccurate, the individual must submit the request in writing to vlm@va.gov, specify the information that should be corrected, and provide a reason to support the request for amendment. All amendment requests should be submitted to the NCA via VLM Customer Support phone (866-245-1490) or email (vlm@va.gov). In accordance with the VLM User Policy, the VA makes no claim to the accuracy of user-submitted information.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

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

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

Follow the format below:

Privacy Risk: There is a risk that incorrect information is published.

Mitigation: Modifications to NCA-data in a deceased Veteran's profile should be submitted to NCA via VLM Customer Support phone (866-245-1490) or email (vlm@va.gov).

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?

VLM administrative actions are reserved to the NCA Admin Role. NCA will assign a limited amount of people with VLM NCA Admin Role. NCA Management will approve and assign the NCA personnel to the NCA Admin Role.

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?

Users from other agencies do not have access to any VLM data.

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.

Data manipulation is controlled by 2-factor authentication Role-Based access to the system. Access is controlled by management.

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.

All contractors have assigned NDAs and Contractor Rules of Behavior and will have access to the system and to PII in the course of their duties. The datastore is accessible by the VA and Contractors. The contractor is responsible for the design, development, and administration of the VLM systems and application.

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 who will be accessing information systems must annually read and acknowledge their receipt and acceptance of the VA Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the VistA Audit user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance obtained through electronic acknowledgment is tracked through the TMS system. All VA employees must complete annual Privacy and Security training. This training includes the following TMS Courses: • VA 10176: Privacy and Info Security Awareness and Rules of Behavior • VA 10203: Privacy and HIPAA Training • VA 3812493: Annual Government Ethics

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Current
2. *The System Security Plan Status Date:* 12/27/2023
3. *The Authorization Status:* 3 Year ATO
4. *The Authorization Date:* 2/16/2021
5. *The Authorization Termination Date:* 12/14/2024
6. *The Risk Review Completion Date:* 12/27/2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Low classification

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.***

<<ADD ANSWER HERE>>

Section 9 – Technology Usage

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

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

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

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

VA Enterprise Cloud (VAEC) – Infrastructure as a Service (IaaS)

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.*

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.

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.

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).

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 provided in this Privacy Impact Assessment is true and accurate.

CYNTHIA MERRITT

Digitally signed by CYNTHIA MERRITT
Date: 2024.03.04 08:45:27 -05'00'

Privacy Officer, Cindy Merritt

RONALD COX

Digitally signed by RONALD COX
Date: 2024.03.04 10:51:49 -06'00'

Information Systems Security Officer, Ronald Cox

ERIN FINCHAM

Digitally signed by ERIN FINCHAM
Date: 2024.03.04 12:23:58 -05'00'

Information Systems Owner, Erin Fincham

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).

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