Privacy Impact Assessment for the VA IT System called:

Memorial Enterprise Letters (MEL) AWS

National Cemetery Administration (NCA)

Business Transformation & Requirements Services (BTRS)

eMASS ID 1072

Date PIA submitted for review:

12/04/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Cynthia Merritt	Cindy.Merritt@va.gov	321-200-7477
Information System Security Officer (ISSO)	Kehinde Talabi	Kehinde.Talabi@va.gov	202-340-8970
Information System Owner (ISO)	Sathish Kadiresan	Sathish.Kadiresan@va.gov	206-495-8214

Abstract

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

The Memorial Enterprise Letters (MEL) Amazon Web Services (AWS) project establishes the National Cemetery Administration's (NCA) ability to build new letter templates and automate business rules for template approval by replacing the legacy custom application (a.k.a. "Resolution Letters") with a configurable lightweight correspondence engine. MEL generates denial letters or solicits additional information in response to a request for a VA Headstone, Marker, or Medallion. The MEL application eliminates NCA's dependency on Information Technology (IT) support for letter template creation or edits and positions NCA to be better able to integrate with a VA enterprise-wide correspondence application when selected. Implementation of the MEL application is one step in the on-going process of modernizing the NCA mission-critical applications.

Overview

The overview is the most important section of the Privacy Impact Assessment (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 business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?

The MEL lightweight correspondence engine (LCE) solution provides the National Cemetery Administration (NCA) more control over the management of official correspondence templates through the use of editor capabilities for creating, updating, and deleting templates without needing to engage Information Technology (IT) for support. It provides the NCA with accurate and timely statistical reports that detail the numbers of letters generated, site and user-specific letter activities, and location where letters were printed (i.e. locally or at a central facility). The letter recipient, which may include the applicant, consignee, or cemetery, benefit by receiving accurate, appropriate, and timely correspondence regarding their request or appeal for a Memorial Benefit.

B. Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.

This is VA owned and non-VA operated system. The MEL System Owner is Sathish Kadiresan. The system is sponsored by the office of Business Transformation & Requirements Services (BTRS). The Business Owner is William Rodgers, Product Line Manager (Acting).

2. Information Collection and Sharing

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

Veteran or Dependents: MEL processes approximately 360,000 applications per year via the Automated Monument Application System (AMAS).
VA Employees: 85 accounts
VA Contractors: 6 accounts

Check if Applicable	Demographic of Individuals
☒	Veterans or Dependents
☒	VA Employees
☐	Clinical Trainees
☒	VA Contractors
☐	Members of the Public/Individuals
☐	Volunteers

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

MEL collects PII about Veterans or Dependents and contact information to generate letters while suspending or denying an application for a government headstone, marker, or medallion. The NCA Case Managers use the templates to create letters to the next of kin or cemetery explaining why their application for the government headstone, marker, or medallion has been suspended or denied.

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

MEL interfaces with the Automated Monument Application System (AMAS) which contains the case management data required for the MEL system to generate letters. Users cannot update the information provided on the Veteran Details screen as the fields showing the data are read-only. MEL retrieves the case data directly from the AMAS database to update the letter status and the final PDF copy of the letter is returned to AMAS.

F. Are the modules/subsystems only applicable if information is shared?

MEL doesn't contain any modules or subsystems.

G. Is the system operated in more than one site to include primary and secondary 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?

This Enterprise Letters capability interfaces with the Federal Information Processing Standards (FIPS) 199 Moderate categorized Automated Monument Application System (AMAS) for information. In the case of Resolution Letters specifically, the information that was submitted on the 1330 application is stored in the AMAS-side of the Burial Operations Support System (BOSS) Enterprise database and stored in the record of correspondence in the Feith Document Database (FDD). Once the letters are complete, they will be sent to the Print Vendor for printing and mailing. There is also an option for printing the letter locally.

3. Legal Authority and System of Record Notices (SORN)

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

Title 38, United States Code, Sections 501(a), 1705, 1710, 1722, and 5317
48VA40B, *Veterans (Deceased) Headstone or Marker Records -VA* (5/9/2023), per Title 38, United States Code: Sections 501(a), 501(b), and Chapter 24, Sections 2400-2404
https://www.govinfo.gov/content/pkg/FR-2023-05-09/pdf/2023-09838.pdf

H. What is the SORN?

48VA40B, *Veterans (Deceased) Headstone or Marker Records -VA* (5/9/2023)
https://www.govinfo.gov/content/pkg/FR-2023-05-09/pdf/2023-09838.pdf

I. SORN revisions/modification

SORN 48VA40B was last updated on May 9, 2023.

I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval.

The system is not in the process of being modified.

4. System Changes

J. Will the business processes change due to the information collection and sharing?

☐ Yes
☒ No

K. Will the technology changes impact information collection and sharing?

☐ Yes
☒ No

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 Information 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
- ☒ **Full** Social Security Number
- ☐ **Partial** 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/Sex
- ☐ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☒ Date of Death
- ☐ Business Email Address
- ☐ Electronic Data Interchange Personal Identifier (EDIPI)
- ☒ Other Data Elements (List Below)

Other PII/PHI data elements: Service Number, VA User ID

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

1.2 List 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?

This Enterprise Letters capability will be accomplished by interfacing with the Automated Monument Application System (AMAS) for information. In the case of Resolution Letters specifically, the information that was submitted on the 1330 Form application is stored in AMAS database and stored in the record of correspondence in the Feith Document Database (FDD). VA Form 1330 uses the VA system of records notice, 48VA40B, published in the Federal Register.

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.

Information is collected from AMAS rather than from the individual because the Veteran is deceased and not able to provide their personal information.

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

Yes, MEL creates information in the form of a letter in regard to an application for a government headstone, marker, or medallion. AMAS and FDD are components of the BOSS Enterprise. The BOSS Enterprise comprises multiple systems including BOSS, Monument Application Scanning System (MASS), First Notice of Death (FNOD), Cemetery Kiosk and Nationwide Gravesite Locator (KNGL), Presidential Memorial Certificate (PMC), and Gravesite Assessment and Reporting (GAR). In short, BOSS Enterprise is NCA's electronic system for decedent burial information supporting documents, eligibility research, interment schedules; and headstone, marker, and medallion data related to the interments. The term BOSS, in this document, refers to the BOSS Enterprise as a whole. This includes the BOSS Enterprise database which consists of BOSS (burial benefits processing) and AMAS (memorial benefits processing) data co-joined. AMAS - An AMAS User receives a Monument Application for a government headstone or marker and evaluates the information on the application. If there is an issue with the Monument Application, the AMAS User will deny or suspend the request and create a Resolution Letter explaining the reason for that decision.
Enterprise Letter - Typically, a Case Manager will initiate the Letter via internal MEL Workflows and access the existing resolution Letter Templates from the MEL internal database. These are presented back to the Case Manager and a selection is then made. Letter data begins to be auto populated and mandatory and optional enclosures are attached to the letter. The Case Manager can preview the state of the letter as progress is made through the workflow utilizing the correspondence engine to generate in-progress or completed letters in Portable Document Format (PDF) format. All working letters, as well as final letters and status, are recorded in the

MEL internal database. Additional capabilities exist in the form of creating scheduled and ad hoc reports regarding the work completion, status, and backlog for processing. These reports will be available in several formats (text, Comma Separated Values (CSV), and PDF) as the requestor determines the need.

1.3 Methods of information collection

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?

MEL receives information from the 1330 Form stored in the AMAS side of the BOSS Enterprise database and also stored in the record of correspondence in the Feith Document Database (FDD).

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?

Information for MEL is collected via form VA40-1330. The OMB Control number is No. 2900-0222.

1.4 Information checks for accuracy, and 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.

MEL does not perform data quality checks. AMAS is ultimately responsible for the accuracy of data and documents.

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?

The MEL application uses JPA/Hibernate Entities to ensure that data corruption has not occurred. JPA/Hibernate Entities are used to hold the data that comes from the AMAS database and will have the data conform to the columns and data types specified in the java entity. If the value received from the entity does not conform to the data structure of the java entity, then MEL will throw an error.

1.5 Identify the specific legal authorities, arrangements, and agreements that 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

MEL will adhere to the VA Directive 6508, Personally Identifiable Information (PII). A subcategory of VA Sensitive Data, PII means any information about the individual maintained by an agency including but not limited to the following: (i) education, financial transactions, medical history, and criminal or employment history; (ii) Information that can be used to distinguish or trace the individual's identity, including name, social security number, date and place of birth, mother's maiden name, biometric records or any other personal information which is linked or linkable to an individual. This term can be interchanged with Sensitive Personal Information (SPI) and Office of Management and Budget (OMB) Memorandum M-03-22

Information in identifiable form is information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors. A Memorandum of Understanding (MOU) and Memorandum of Agreement (MOA) will be developed if applicable. The MEL legal authorities, Federal laws, regulations, statutes, and Executive Orders are:

- Executive Order 9397, Numbering System for Federal Accounts Relating to the Individual Persons
- Executive Order 13478, Amendment to Executive order 9397 Relating to Federal Agency Uses of Social Security Numbers (Nov.2008) • Title 38 of U.S. Code Section 1705(c) (1)(2)
- Pub. L. 104-262, SEC 104. Management of Health care, SEC 1705. Management of Health care: patient enrollment system. SEC 1706 Management of Healthcare: other requirements (a) (b) (1) • 5 U.S.C. 552a, "Privacy Act," c. 1974
- 5 U.S.C. 552, "Freedom of Information Act," c. 1967 • HIPAA Privacy Rule, 45 C.F.R. Part 164, Standards for Privacy of Individually Identifiable Health Information
- VA Claims Confidentiality Statute, 38 U.S.C § 5701
- Confidentiality of Certain Medical Records, 38 U.S.C. § 7332
- Federal Information Security Management Act (FISMA) of 2002
- OMB M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
- The Freedom of Information Act, as amended 5 U.S.C. 552
- VA Directive Handbook 6500 Risk Management for VA Information Systems
- VA Directive and Handbook 6502, Privacy Program

- VA Directive 6508, Implantation of Privacy Threshold Analysis and Privacy Impact Assessment
- VA Directive 2012-035.on Reduction of the Use and Collection of SSN
- VHA Directive 1906, Data Quality Requirements for Healthcare Identity Management and Master Veterans Index Functions
- Federal Information Processing Standard (FIPS) 199
- National Institute of Standards and Technology (NIST) SP 800-60

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: The collection ties with the purpose of the underlying mission of the organization and its enabling authority.

Principle of Minimization: The information is directly relevant and necessary to accomplish the specific purposes of the program.

Principle of Individual Participation: The program, to the extent possible and practical, collects information directly from the individual.

Principle of Data Quality and Integrity: VA policies and procedures must ensure that personally identifiable information is accurate, complete, and current.
This 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 significant risk if the privacy related data contained in MEL is intentionally or unintentionally disclosed. The deceased's identity could be stolen causing harm to descendants and family. Disclosure of PII/PHI could cause embarrassment or pain to friends and family of the deceased as well.

Mitigation: MEL is designed to meet all VHA Security, Privacy, and Identity Management requirements including VA Handbook 6500 (see Appendix E and Appendix F). MEL is designed to comply with the applicable approved Enterprise Service Level Agreement (SLA). Additionally, the Department of Veterans Affairs is careful to only collect the information necessary to determine eligibility of those Veterans and dependents that file claims. By only collecting the minimum necessary information to process each request, the VA can better protect the individual's information. Records are only released only to authorized VSRs working the claim. The Department of Veterans Affairs applies consistent security guidance to centralize and standardize account management, network access control, database security, vulnerability scanning and remediation.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
Name	Used to identify Veterans, spouses, and Next-of-Kin	Not used
Full Social Security Number	Used to verify Veteran identity and eligibility	Not used
Date of Birth	Used to verify Veteran identity and eligibility	Not used
Date of Death	Used to verify Veteran identity and eligibility	Not used
Personal Mailing Address	Used to determine location of decedent and Next-of-Kin	Not used
Personal Phone Number	Used to verify Veteran identity and eligibility	Not used
Personal Email Address	Used to verify Veteran identity and eligibility	Not used
Service Number	Used to verify Veteran identity and eligibility	Not used
VA User ID	Used to verify Veteran identity and eligibility	Not used

2.2 Describe the types of tools 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?

MEL application creates a record every time a new letter is created for a case. Once the letter is completed and printed, this record will be transmitted to AMAS. MEL application has built-in features to schedule and execute reports to measure the performance of a Site or a User.

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.

Case Data from the AMAS system is utilized to generate letters in MEL. Letters are customized, modified, and submitted by an author such as a Case Manager, Team Leaders, and Site Supervisors. When a letter is generated, a workflow is used to review, edit, approve, and return the proposed letter. This workflow creates a record within MEL. The letter is then printed and mailed to the Veteran's family. The information created as part of the workflow is stored within MEL and is accessible by the system users who make the determinations about the submitted application for the Monument.

2.3 How the information in the system is 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?

The MEL database is encrypted using Amazon Web Services (AWS) Key Management Service (KMS) with
Advanced Encryption Standard (AES) algorithm in Galois/Counter Mode (GCM) with 256-bit secret keys for data at rest. While Social Security Numbers (SSNs) may be used to identify individuals in AMAS, they do not appear in any letters created by the MEL application. Secure Socket Layer (SSL), Transport Layer Security (TLS), and Hypertext Transfer Protocol Secure (HTTPS) are used for encrypting data in transit.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? (refer to PTA question 3.8).

MEL system access is controlled through various user roles. Each role has limited access to specific modules of the system. These roles serve as additional protection imposed to SSNs as well as the entire system. Additionally, the database is strictly controlled by a Database Administrator (DBA) role assigned to the administrators which not only protects the SSNs but also the entirety of MEL's data. The same is applicable on the AMAS system.

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

MEL follows the Incident Response Plan (IRP) Guidelines and Directives set forth by the VA including reporting of security incidents as mentioned in OMB Memorandum M-06-15.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

NCA staff must complete appropriate trainings and receive approval from management before they are given approval to be provisioned. Required Talent Management System (TMS) Trainings include Privacy Training and Rules of Behavior Training.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented? How are the documented, i.e. Policy, SOP, other. And where is this documentation located?

Yes, criteria, procedures, controls, and responsibilities regarding access are documented in the MEL Access Control (AC) Standard Operating Procedures (SOP). This Access Control SOP is stored in the VA's Governance, Risk and Compliance (GRC) tool known as Enterprise Mission Assurance Support Service (eMASS). All personnel responsible for MEL also retain a copy of the AC SOP.

2.4c Does access require manager approval?

Yes, access requires manager approval.

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

Yes, via provisioning forms, manager approval, and via Service Now (SNOW) tickets requesting access. Approvals are granted by Office of Information Technology (OIT) in conjunction with the Business Owner. Additionally, the security controls for MEL are in place to ensure data is used and to protect the Confidentiality, Integrity, and Availability of VA information systems and the information processed, stored, and transmitted by those systems. Controls include mandatory training completion for all employees, volunteers, and contractors. Additionally, audits are performed to ensure information is accessed and retrieved appropriately.

2.4e Who is responsible for assuring safeguards for the PII as identified in eMASS?

VA and MEL have implemented required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 Rev. 5 and VA Directive &

Handbook, VA Handbook 6500, Risk Management Framework for VA Information Systems. Per the approval of the Acting Assistant Secretary for information Technology (the VA Designated Accrediting Authority [DAA]), the MEL AWS Information System Owner is responsible for assuring safeguards for the PII. The application team has implemented the required security controls based on tailoring guidance of NIST Special Publication 800-53 Rev 5, NIST SP 800-53B and VA directives and handbooks. VA Records Management Policy and VA National Rules of Behavior in the Talent Management System govern how Veterans' information is used, stored, and protected.

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*

MEL will collect and retain Veteran or decedent name, social security number, date of birth, date of death, and mailing address. This information can be found on the VA Form 1330.

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 https://www.archives.gov/records-mgmt/grs? This question is related to privacy control DM-2, Data Retention and Disposal.*

The NCA Privacy Office and NCA Records Officer shall be consulted to ensure that appropriate retention and destruction schedules are implemented for MEL. All MEL records will be maintained in accordance with VA Records Control Schedule (RCS) 10-1. Therefore, they are retained for 75 years. All PII will be disposed of at the end of the retention period as required by law or regulation.

3.3 The retention schedule 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. Please work with the system 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 records are stored within MEL except the Case Data which is pulled from the AMAS system.

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

The NCA Privacy Office and NCA Records Officer shall be consulted to ensure that appropriate retention and destruction schedules are implemented for MEL. All MEL records will be maintained in accordance with 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.

Electronic data and files of any type, including PHI, SPI, Human Resources records, and more are destroyed in accordance with the Media Sanitization section of the VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and are compliant with NIST SP 800-88. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle Bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction.

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.

MEL has a policy to only use real PII data in the production environment where access is limited to those who have a business need to use the PII. All the MEL test environments use fictitious data. Since all testing and training are performed in the MEL test environments, we use only fictitious data for these activities. The MEL users can generate reports in the production environment to perform research. However, none of the reports available in the MEL application contain PII.

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 Privacy Officer (PO) 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: The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.

Principle of Data Quality and Integrity: The PIA should describe 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: There is a risk that the archived data may be retained longer than necessary. Records, especially those containing Personally Identifiable Information (PII) or Sensitive Personal Information (SPI) that are retained longer than required are at a greater risk of unauthorized access, privacy or security breach. This also increases the risk that an individual's information may be accessed by those without a need-to know.

Mitigation: The National Archives and Records Administration (NARA) will dispose of records in accordance with NARA's guidelines. Therefore, information will only be kept in compliance with VA RCS10-1.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

PII Mapping of Components

4.1a Memorial Enterprise Letters AWS consists of 1 key component (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 Memorial Enterprise Letters AWS 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 3.9a 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**
Automated Monument Application System (AMAS)	Yes	Yes	• Name • Full Social Security Number • Service Number • Date of Birth • Date of Death • Personal Mailing Address	The PII used to create the letter for a case that is being denied or suspended.	MEL interfaces with AMAS using direct database access through Java Persistence API (JPA).

4.1b List internal organizations information is shared/received/transmitted, the information shared/received/transmitted, and the purpose, and how the information is transmitted.

NOTE: Question 3.9b (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

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
Memorial Enterprise Letters (MEL) Automated Monument Application System (AMAS)	Automated Monument Application System (AMAS). MEL pulls the veteran case data from AMAS to generate a new letter and also updates AMAS with the letter status.	• Name • Full Social Security Number • Service Number • Date of Birth • Date of Death • Personal Mailing Address	MEL interfaces with AMAS using direct database access through Java Persistence API (JPA).

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the VA network 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 in this section.).

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

Follow the format below:

Privacy Risk: There is a significant risk to the veteran's family if privacy related data contained in MEL is intentionally or unintentionally disclosed. The deceased's identity could be stolen, causing harm to descendants and family. Disclosure of PII/PHI could cause embarrassment or pain to friends and family of the deceased.

Mitigation: MEL is designed to meet all VHA Security, Privacy, and Identity Management requirements including VA Handbook 6500 (see Appendix E and Appendix F). MEL is designed to comply with the applicable approved Enterprise Service Level Agreement (SLA). Additionally, the Department of Veterans Affairs is careful to only collect the information necessary to determine eligibility of those Veterans and dependents that file claims. By only collecting the minimum

necessary information to process each request, the VA can better protect the individual's information. Records are only released only to authorized VSRs working the claim. The Department of Veterans Affairs applies consistent security guidance to centralize and standardize account management, network access control, database security, vulnerability scanning and remediation.

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 List the external organizations (outside VA) that information shared/received. and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.

The sharing of information outside the agency must be compatible with the original collection. The sharing must be covered by an appropriate routine use in a SORN. If not covered, 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 IT System or External Program Office information is shared/received with	***List the purpose of information being shared / received / transmitted***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)***	***List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
N/A	N/A	N/A	N/A	N/A

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: There is no external sharing.

Mitigation: There is no external sharing.

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 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of

the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms, notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.

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 Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.

SORN: Federal Register :: Federal Register Document Issue for 2023-05-09

Privacy Act Notice on Form 40-1330: PRIVACY ACT - VA considers the responses you submit confidential (38 U.S.C. 5701). VA may only disclose this information outside the VA if the disclosure is authorized under the Privacy Act, including the routine uses identified in the VA system of records, 48VA40B, published in the Federal Register. VA considers the requested information relevant and necessary to determine maximum benefits under the law.

6.1b If notice was not provided, explain why.

6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.

PRIVACY ACT - VA considers the responses you submit confidential (38 U.S.C. 5701). VA may only disclose this information outside the VA if the disclosure is authorized under the Privacy Act, including the routine uses identified in the VA system of records, 48VA40B, published in the Federal Register. VA considers the requested information relevant and necessary to determine maximum benefits under the law.

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.

This is not applicable to the system. MEL uses the data collected by AMAS. AMAS and FDD are components of the BOSS Enterprise. The BOSS Enterprise comprises multiple systems, including BOSS, Monument Application Scanning System (MASS), First Notice of Death (FNOD), Cemetery Kiosk and Nationwide Gravesite Locator (KNGL), Presidential Memorial Certificate (PMC), and Gravesite Assessment and Reporting (GAR). In short, BOSS Enterprise is NCA's electronic system for decedent burial information; supporting documents; eligibility research; interment schedules; and headstone, marker, and medallion data related to the interments. The term BOSS, in this document, refers to the BOSS Enterprise as a whole. This includes the BOSS Enterprise database, which consists of BOSS (burial benefits processing) and AMAS (memorial benefits processing) data co-joined. An AMAS User receives a Monument Application for a government headstone or marker and evaluates the information on the application. If there is an issue with the Monument Application, the AMAS User will deny

or suspend the request and create a Resolution Letter explaining the reason for that decision. Therefore, this item does not apply to MEL. The following statement is provided on the VA Form 1330 if the individual declines to provide the requested information: "RESPONDENT BURDEN - Public reporting burden for this collection of information is estimated to average 15 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. VA cannot conduct or sponsor a collection of information unless it has a valid OMB number. Your obligation to respond is voluntary; however, your response is required to obtain benefits. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to the VA Clearance Officer (005R1B), 810 Vermont Avenue, NW, Washington, DC 20420. Please DO NOT send claims for benefits to this address."

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.

Once information is provided to the VA, the records may be used as necessary to ensure the administration of statutory benefits to all eligible Veterans. As such, the MEL system does not provide Veterans with the direct opportunity to consent to particular uses of information. However, if a Veteran wishes to remove consent for a particular use of their information, they should contact the nearest VA regional office, a list of which can be found at http://benefits.va.gov/benefits/offices.asp.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your Privacy Officer (PO) to complete all Privacy Risk questions inside the document this section).

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

Principle of Transparency: This is referring to sufficient notice provided to the individual.

Principle of Use Limitation: The information used only for the purpose for which notice was provided either directly to the individual or through a public notice. The procedures in place must 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 an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by the National Cemetery Administration prior to

providing this information to the NCA for use in systems such as MEL AWS. An individual may not be aware of how the VA collects PII and how it is used internally to create letters while suspending or denying an application for government headstones, markers, or medallions.

Mitigation: The VA mitigates this risk by providing veterans and other beneficiaries with multiple forms of notice of information collection, retention, and processing as discussed in section 6.1 of this form. The main forms of notice are the Privacy Act statement, System of Record Notice (SORN), and the publishing of this Privacy Impact Assessment.

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 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 VA Public Access Link-Home (efoia-host.com) to obtain information about FOIA points of contact and information about agency FOIA processes.***

VA provides Veterans the ability to request their medical records by submitting a VA Form 10-5345a to their VA health facility's medical records or release of information office. A list of regional VA offices may be found at: http://benefits.va.gov/benefits/offices.asp

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)?

MEL is not exempt from access provisions of the Privacy Act.

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

MEL is a Privacy Act System.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed? If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

As stated in 7.1, a Veteran can request for Amendment to their information if the information is deemed to be incorrect. Individuals seeking to contest or amend records in MEL

pertaining to them should contact the system manager in writing. A request to contest or amend records must state clearly and concisely what record is being contested, the reasons for contesting it, and the proposed amendment to the record.

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 made aware of the procedures for correcting his or her information through the SORN, the Privacy Act, and this PIA:

SORN: 48VA40B, *Veterans (Deceased) Headstone or Marker Records -VA*
https://www.govinfo.gov/content/pkg/FR-2023-05-09/pdf/2023-09838.pdf
Privacy Act: Privacy, Policies, And Legal Information | Veterans Affairs
PIA: Privacy Impact Assessments (PIA) - Privacy

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.

The Privacy Act as well as the HIPAA Privacy allows for right of access to the Veteran or individual's record as well as making an amendment request. This is done through the local VA facility Privacy Officer. There is a formal redress option in place.
https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=809&FType=2

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 Privacy Officer (PO) to complete all Privacy Risk questions in this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: The individual must be provided with the ability to find out whether a project maintains a record relating to them.

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

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

Follow the format below:

Privacy Risk: There is a risk that Veterans, Spouse, Decedent and Next of Kin may not know the relevant procedures for gaining access to, correcting, or contesting their information.

Mitigation: The privacy risk is mitigated by Notice of Privacy Practice. By publishing this PIA and the applicable SORN, the VA makes the public aware of the unique status of applications and files. Furthermore, this document and SORN provide the point of contact for members of the public who have questions or concerns about applications and files.
https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=404&FType=2

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures. (Work with your ISSO to complete this section).

8.1 The procedures in place to determine which users may access the system, must be 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?

To receive access to MEL, a user must submit a 9957 form which is reviewed by the Application Support Analyst (ASA) team and then by the system Technical Lead, and finally by the MEL stakeholders. Upon approval by the stakeholders, access and permissions are granted to the user by the ASA team.

MEL was designed and developed to meet all VHA Security, Privacy, and Identity Management requirements including VA Handbook 6500 (see Appendix E and Appendix F). MEL was designed and developed to comply with the applicable approved Enterprise Service Level Agreement (SLA).

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 MEL. To receive access to MEL, another system user with appropriate permissions must sponsor the user from another agency. The sponsor will describe the functionality the user needs within MEL, the new user's role, and any security caveats that apply to the user. These roles will be governed by permission sets that allow page/field level control of the information and data. MEL performs Access Control using a Role-Based Access Control (RBAC) model which is built into the system. MEL uses the Function Roles assigned to a user to make authorization decisions regarding resource access at all layers which includes the UI,

data, and service layers. After a user logs in to the system, the application permissions granted to the user allows them to make authorization decisions.

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.

All personnel authorized to access MEL are considered privileged users and are managed, identified, and authenticated in a consistent fashion in accordance with System Security Controls IA-2 and IA-2(1). Each user within MEL is assigned one or more role. A user's role determines what the user can do within the system. The user roles are detailed below:

- View Letter: Users with the View Letter role are authorized to see a PDF preview of any completed letter in MEL by viewing it from the AMAS history screen. Users with the View Letter role can also access their own User Profiles within MEL.
- Case Manager: The Case Manager generates letters to be printed and mailed to the recipient. Case Managers submit completed letters to Team Leaders, Site Supervisors, Alternate Letter Approvers, or NCA Supervisors for approval. In addition, Case Managers can generate reports and view dashboards on their own activities. Lastly, Case Managers can view all completed letters from AMAS regardless of author or site association.
- Alternate Letter Approver: Alternate Letter Approvers are Case Managers granted the authority to edit, approve and electronically sign, or return letters on the behalf of the Site Supervisor. They may also create letters and generate reports and view dashboards on their own work. Lastly, Alternate Letter Approvers can view all completed letters from AMAS regardless of author or site association.
- Team Leader: The Team Leader has the authority to generate letters and to edit and approve or return letters on behalf of the Site Supervisor. Team Leaders can also generate reports and view dashboards on their own work and the work activities of users at their sites. Lastly, Team Leaders can view all completed letters from AMAS regardless of author or site association.
- Site Supervisor: The Site Supervisor manages a Memorial Products Service (MPS) site and has the authority to generate letters and to edit and approve or return letters. Site Supervisors can also generate reports and view dashboards on their own work and the work activities of users at their site(s). Lastly, Site Supervisors can view all completed letters from AMAS regardless of author or site association.
- National Cemetery Administration (NCA) Supervisor: The National Cemetery Administration (NCA) Supervisor manages all the MPS sites and has the authority to generate letters and to edit and approve or return letters for all sites. NCA Supervisors can also generate reports and view dashboards on their own work and on the work activities of users at all sites. They can also edit user profiles across all MPS sites, reset user passwords, and unlock user accounts. Lastly, NCA Supervisors can view all completed letters from AMAS regardless of author or site association.
- Administrator: A MEL Administrator is responsible for maintaining and updating the administration material that supports the generation of letters. An

Administrator has the capability to add and edit letter templates and the constituent parts, such as paragraph boilerplate text, enclosures, logos, letterhead, site information, and standard remarks. Administrators are also responsible for assigning new users and defining roles.

- Print Vendor: The Central Print and Mail Facility (hereafter referred to as the Print Vendor) is responsible for printing and mailing completed letters that are not found to be suspicious. The vendor will return any suspicious letters to the NCA Supervisor to reissue. They may also generate dashboards to get an overview of work performance at the central print and mail facility.

8.2a. Will VA contractors have access to the system and the PII?

Yes, VA contractors have access to MEL. The Contracting Officer Representative (COR) approves all new or modified incoming or outgoing contracts involving MEL. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of Behavior training via the VA's Talent Management System (TMS). The office of Contract Review operates under a reimbursable agreement with VA's Office of Acquisition, Logistics and Construction (OALC) to provide pre-award, post-award, and other requested reviews of vendors' proposals and contracts.

VA contract employee access is verified through authorized VA personnel before access is granted to any contractor. Contracts and contractor access are reviewed annually. All contractors are cleared using the VA background investigation process and must obtain the appropriate background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access.

8.2b. What involvement will contractors have with the design and maintenance of the system?

Design and maintenance is conducted via contractors for MEL with OIT Business approval.

8.2c. Does the contractor have a signed confidentiality agreement?

No, a confidentiality agreement is not signed. VA contract employees access is verified through the Contracting Officer's Representative (COR) and other VA supervisory/ administrative personnel before access is granted to any VA system. Contractor access is reviewed annually at a minimum. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via the VA Talent Management System (TMS). All contractors are vetted using the VA background investigation process and must obtain the appropriate level background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access. Generally, contracts are reviewed at the start of the initiation phase of acquisitions and again during procurement of option years by the Contracting Officer, ISSO, Privacy Officer, COR, Procurement Requestor/Program Manager and any other stakeholders required for approval of the acquisition.

8.2d. Does the contractor have an implemented Business Associate Agreement for applicable PHI?

No, contractors do not have an implemented Business Associate Agreement for applicable PHI as MEL does not contain PHI. MEL does not contain medical records or files.

8.2e. Does the contractor have a signed non-Disclosure Agreement in place?
If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.

Contractors do not sign a Non-Disclosure Agreement.

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

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

All personnel with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually. In addition, user manuals and training tools shall be developed. If they already exist, updates shall be made, as necessary, to them and they shall be delivered to all levels of users.

8.4 The Authorization and Accreditation (A&A) completed for the system.

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* August 28, 2024
3. *The Authorization Status:* Approved Authorization to Operate (ATO)
4. *The Authorization Date:* November 6, 2024
5. *The Authorization Termination Date:* September 27, 2026
6. *The Risk Review Completion Date:* September 27, 2024
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

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

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. ***(Refer to question 1.8 of the PTA)***

MEL is hosted in the VAEC AWS GovCloud.

9.2 Does the contract with the Hosting 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 3.3.1 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 they provided in this Privacy Impact Assessment is true and accurate.

CYNTHIA MERRITT

Digitally signed by CYNTHIA MERRITT
Date: 2024.12.30 11:19:31 -05'00'

Privacy Officer, Cynthia Merritt

KEHINDE TALABI

Digitally signed by KEHINDE TALABI
Date: 2024.12.30 13:53:24 -05'00'

Information System Security Officer, Kehinde Talabi

SATHISH KADIRESAN

Digitally signed by SATHISH KADIRESAN
Date: 2024.12.30 05:48:15 -08'00'

Information System Owner, Sathish Kadiresan

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).

VA Form 40-1330, CLAIM FOR STANDARD GOVERNMENT HEADSTONE OR MARKER.

Privacy Act Notice on Form 40-1330: PRIVACY ACT - VA considers the responses you submit confidential (38 U.S.C. 5701). VA may only disclose this information outside the VA if the disclosure is authorized under the Privacy Act, including the routine uses identified in the VA system of records, 48VA40B, published in the Federal Register. VA considers the requested information relevant and necessary to determine maximum benefits under the law.

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

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 Directive 1605.04
IB 10-163p (va.gov)