Privacy Impact Assessment for the VA IT System called:

Memorial Benefits Management System (MBMS)

Office of Information and Technology (OIT)
National Cemetery Administration (NCA)

Date PIA submitted for review:

September 27, 2022

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)	Joseph Facciolli	Joseph.Facciolli@va.gov	(215) 842-2000 x2012
Information System Owner	Michael Ouslander	Michael.Ouslander@va.gov	(817) 999-6851

Abstract

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

The Memorial Benefits Management System (MBMS) serves customers in National Cemetery Administration (NCA) and their partners. MBMS modernized the business system platform and operational processes that support the delivery of memorial and burial benefits to Veterans and their families.

Overview

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

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

Memorial Benefit Management System (MBMS) serves NCA customers and partners. The system is being built and managed by the Office of Information and Technology (OIT).

MBMS provides a platform for the National Cemetery Scheduling Office (NCSO), NCSO Eligibility Office, and National Cemetery Operations staff (directors, office personnel, grounds foremen, grounds crews) to serve Veterans and their families through eligibility verification, scheduling, and burial operations.

Eligible Veterans and family members are buried in the 135+ National Cemeteries managed by NCA every year. Both Veterans and their spouses are served and MBMS services Veterans, spouses, or Next of Kin (NOK) as they request eligibility verification and service scheduling at the nation's National Cemeteries. In addition, memorials are processed each year and shipped to private cemeteries for NOK. There are approximately 50,000 individuals, including Veterans, spouses and NOK, whose information is in MBMS.

MBMS is a national system accessible from the VA network at the NCSO and each National Cemetery. The initial phases focused on the Field Programs workstream, but ultimately, all three of the NCA pillars will be serviced by MBMS. Initial delivery falls under the Office of the Deputy Under Secretary for Field Programs and Cemetery Operations, while the end state will fall under the Office of the Under Secretary for Memorial Affairs (40).

MBMS contains information supporting Veteran and Next-of-Kin burial service eligibility determination as well as service scheduling information. PII in the form of Veteran's and Next-of-Kin's data including Name, Social Security Number (SSN), Birth Date, Date of Death, Gender, Marital Status, and Address of Record. Veteran Data to include Name, SSN, Birth Date, Date of Death, Gender, Marital Status, Address of Record, Military Service Number, Military Service Entered on Duty (EOD) Date, Military Service Release from Active Duty (RAD) Date, Veteran's Period of Service, and Veteran's War Period. In addition, non-sensitive information pertaining to funeral homes, decedents, and Veterans will be captured, transmitted, and stored.

The MBMS Case Management module, located in VA Salesforce, will share information for the following subsystems with the MBMS Bulk Case Queue and Cemetery Management modules hosted on MBMS in VA Enterprise Cloud (VAEC) Amazon Web Services (AWS) on the Benefits Integration Platform (BIP): Case Management (Self Service Case Queue, Case Intake, and Eligibility Verification) to Bulk Case Queue (Queue Management and Case Queue) Case Management (Scheduling) to/from Cemetery Management (Schedule Availability and Regulations Management).

MBMS is operated in a single instance of the VAEC AWS GovCloud, deployed across three Availability Zones.

- Title 38, United States Code, Sections 501(a), 1705, 1710, 1722, and 5317
- 48VA40B – Veterans (Deceased) Headstone or Marker Records -VA, per Title 38, United States Code: Sections 501(a), 501(b), and Chapter 24, Sections 2400-2404
- Information from the SORN: 38 U.S.C. 501(a); 38 U.S.C. 73; 38 U.S.C. 75 SEC 4202; 5 U.S.C. Part III, Subparts D and E
- 5 U.S.C. 552, "Freedom of Information Act," c. 1967
- 5 U.S.C. 552a, "Privacy Act," c. 1974
- OMB Circular A-130, Appendix III, "Security of Federal Automated Information Systems"
- Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act)
- 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"
- VA Directive and Handbook 6502, Privacy Program

Completion of this PIA will not result in circumstances requiring changes to business processes.

Completion of this PIA is not anticipated to result in technology changes.

MBMS leverages the VAEC Cloud Service Provider (CSP) AWS GovCloud, which is FEDRAMP approved, under the BIP Assessing ATO. Per the approval of the Deputy Assistant Secretary, Enterprise Program Management Office (EPMO) [the VA Authorizing Official (AO)], BIP has an ATO for one calendar year, effective January 6, 2022. VA Business Stakeholders of the BIP minor applications have ownership rights over data. NCA will have rights over MBMS data.

Security and privacy data held by a cloud provider is still required to meet the requirements under the privacy act. Federal agencies are required to identify and assess the risk to their PII, and to ensure security controls are implemented to provide adequate safeguards. Section C MM. of the contract references OMB Memorandum “Security Authorization of Information Systems in Cloud Computing Environments” FedRAMP Policy Memorandum.

Section 1. Characterization of the Information

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

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

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

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.

This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

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

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

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

Additional information collected but not listed above:

- Service Information
- Benefit Information
- Relationship to Veteran
- Funeral Information
- Date of Death
- Marital Status

PII Mapping of Components

MBMS consists of three key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by MBMS, and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

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

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
BOSS_db	Yes	Yes	PII in the form of Veteran's and Next-of-Kin's data including Name, SSN, Birth Date, Date of Death, Gender, Marital Status, and Address of Record. Veteran Data to include Name, SSN, Birth Date, Date of Death, Gender, Marital Status, Address of Record, Military Service Number, Military Service Entered on Duty (EOD) Date, Military Service Release from Active Duty (RAD) Date, Veteran's Period of Service, and Veteran's War Period	Eligibility determination, case tracking, and management through case life cycle	All employees with access to Veteran's information are required to complete the VA Privacy, Information Security Awareness training and Rules of Behavior annually.

Salesforce_db	Yes	Yes	PII in the form of Veteran's and Next-of-Kin's data including Name, SSN, Birth Date, Date of Death, Gender, Marital Status, and Address of Record. Veteran Data to include Name, SSN, Birth Date, Date of Death, Gender, Marital Status, Address of Record, Military Service Number, Military Service Entered on Duty (EOD) Date, Military Service Release from Active Duty (RAD) Date, Veteran's Period of Service, and Veteran's War Period	Eligibility determination, case tracking, and management through case life cycle	All employees with access to Veteran's information are required to complete the VA Privacy, Information Security Awareness training and Rules of Behavior annually.

MPI	Yes	Yes	Veteran Data to include Name, Social Security Number (SSN), Date of Birth (DOB), Gender, Phone Number	Verification for Veteran contact info. It is the authoritative contact data source for the Verified Veteran contact	All employees with access to Veteran's information are required to complete the VA Privacy, Information Security Awareness training and Rules of Behavior annually.

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

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

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

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

MBMS leverages:

- Identity and Access Management (IAM) Single Sign-On Internal (SSOi) and User Provisioning: MBMS Salesforce and AWS uses two VA IAM services to validate user login information: SSOi and User Provisioning.
- Veterans Benefits Management System (VBMS) eFolder via iHub: Provides access to a widget allowing NCSO case managers the ability to view documents in eFolder to assist in eligibility verification of Veterans and Next-of-Kin. The data viewed is viewed for eligibility determinations and not transmitted or stored in MBMS Salesforce or AWS.
- VA Master Persons Index Enterprise (MPIe): Provides the ability to search the authoritative data source for Veterans, MPI, to ensure that they are not creating duplicate contact records in applications built on the Salesforce platform.
- Direct conversation with individual Veterans or NOK who call the NCSO representatives.

1.3 How is the information collected?

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

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

Information is collected through direct phone calls to the NCSO and input into MBMS or cemeteries or entry and submittal of the Pre-Need or Time-of-Need forms found on the Vets.gov website. Forms and supporting documentation required to verify memorial benefits eligibility, such as the DD214, are scanned/uploaded and kept in a VBMS eFolder.

User login and access credentials are collected from IAM SSOi and User Provisioning.

The Digital Veteran's Platform (DVP) is a middleware that integrates VA Enterprise Case Management Solutions System (VECMS) with various backend databases. MPI is one of those databases. DVP will expose a set of APIs (application programming interface), in OpenAPI format, to VECMS via VA Trusted Internet Connection (TIC) complying with MPI's published Enterprise Design Pattern. A gateway in Veterans Health Information Systems and Technology Architecture (VistA) establishes connectivity between the VA Medical Center (VAMC) systems, and links to the MPI for identification.

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

Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.
If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

Standard operating procedures (SOPs) are in place at the NCSO and each cemetery to perform quality control on data related to each case. As cases progress through the queues from NCSO case managers to cemetery office staff, additional data integrity checks are conducted. Final data integrity checks are performed by cemetery operations staff who perform the interment after services.

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.

The MBS operates under the following regulations, statutes, and/or legal citations:

- 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
- 48VA40B – Veterans (Deceased) Headstone or Marker Records-VA, per Title 38, United States Code: Sections 501(a), 501(b), and Chapter 24, Sections 2400-2404.
- Public Law 100---503, Computer Matching and Privacy Act of 1988
- Privacy Act of 1974; U.S Code title 5 USC section 301 title 38 section 1705, 1717, 2306-2308 & Title38, US Code section 7301 (a) and Executive Order 9397
- OMB Circular A---130, Management of Federal Information Resources, 1996
- OMB Memo M---10---23, Guidance for Agency Use of Third---Party Websites
- 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
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- State Privacy Laws
- The legal authority is 38 U.S.C 7601-7604 and U.S.C 7681-7683 and Executive Order 9397

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

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

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

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

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

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

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: MBMS collects SPI on deceased Veterans and limited contact information from their Next of Kin/point of contact for arranging the burial. If this information was breached or accidentally released to inappropriate parties or the public, it could result in potential personal and/or emotional harm to the friends/relatives of the individuals whose information is contained in the system.

Mitigation: The Department of Veterans Affairs is careful to only collect the information necessary to identify the recipients of memorial benefits and process their interment and memorial requests. This involves a review process to identify potential inconsistencies or other issues. By only collecting the minimum necessary information to process each request, the VA can better protect the individual's information. Records are only released to individuals authorized to coordinate interments on behalf of the deceased person (generally, the Next of Kin) upon receipt of proper identification.

The Department of Veterans Affairs applies consistent security guidance to centralize and standardize account management, network access control, database security, vulnerability scanning and remediation. The NCA Information Security Officer is responsible for administering the VA Information Security Programs at NCA facilities, to help them maintain compliance with federal security requirements and VA security policies. This operational security posture maintains and safeguards system information from threats.

Section 2. Uses of the Information

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

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

Identify and list each use (both internal and external to VA) of the information collected or maintained.

This question is related to privacy control AP-2, Purpose Specification.

- Name: Used to identify Veterans, spouses, and next-of-kin
- Social Security Number (SSN): Used to verify Veteran identity and eligibility
- Date of Birth: Used to verify eligibility and memorialization on headstones or markers

- Date of Death: Used to verify spousal and beneficiary relationship to Veteran, at time of death
- Marital Status: Used to verify spousal and beneficiary eligibility
- Mailing Address and Zip Code: Used to determine location of decedent and next-of-kin
- Phone Number: Used to contact points-of-contact
- Fax Number: Used to contact points-of-contact
- Email Address: Used to contact points-of-contact
- Emergency Contact: Used to contact points-of-contact
- Service Information: Used to verify eligibility
- Benefit Information: Used to verify burial benefits
- Relationship to Veteran: Used to determine relationship to Veteran
- Funeral Home Information: Used to contact funeral home or other service coordinator information
- Military Service Information: Used to determine eligibility
- Date of Death: Used to memorialize on headstones or markers
- Gender: Used to verify identity

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

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

If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

MBMS does not perform any kind of analysis or run analytic tasks. The system captures and feeds data to data warehouses and repositories. System applications, such as Tableau, are used to pull that data for analysis. The information is used to determine eligibility and provide services and benefits to Veterans and their beneficiaries by NCA employees.

2.3 How is the information in the system secured?

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

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?
2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?

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

The following applies to both transmission confidentiality and information at rest: MBMS uses AWS built-in encryption for databases. AWS is using AES-256 which is FIPS 140-2 compliant. More information can be found at the AWS website. MBMS is also leveraging an existing connection established between MPI and Salesforce VA. This connection is maintained by the Digital Transformation Center (DTC). DTC manages our account for Salesforce.

The confidentiality and integrity of data communication between MBMS and other parties are guaranteed using Transport Layer Security/Secure Sockets Layer (TLS/SSL) between the communicating nodes at the Transport layer. Users access MBMS through an HTTPS link. Communication between MBMS and IAM SSOi servers is done using mutual (2-way) SSL. This secure communication occurs for all environments from Development through Production.

The VA certificate authority issues digital certificates that contain a public key bound to all MBMS application servers' identities. Similarly, a VA-issued certificate is bound to each endpoint except VA Salesforce. Non-VA certificate authority (CA) is required for the Salesforce endpoint. For example, MBMS and the IAM SSOi endpoint will exchange digital certificates during the handshake procedure. After the handshake procedure concludes and the secured connection begins, AWS makes its requests. Responses to those requests will be encrypted and decrypted using public-key cryptography.

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

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

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

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

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?

This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

The SORN defines the information collected from Veterans, use of the information, and how the information is accessed and stored. The information collected is used for determining a Veteran's burial and monument benefits.

The security controls for MBMS 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. VA and Salesforce have implemented required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 Rev 4 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)].

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

Identify and list all information collected from question 1.1 that is retained by the system.

This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

- Name
- Social Security Number
- Date of Birth
- Date of Death
- Mailing Address
- Zip Code:
- Phone Number
- Fax
- Email Address
- Emergency Contact
- Service Information
- Benefit Information
- Relationship to Veteran
- Funeral Information
- Military service information
- Name and address of Next-of-Kin

- Military service data, applicant's name and address, place of burial, burial services and headstone data
- Gender
- Ethnicity/Race

3.2 How long is information retained?

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

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.

This question is related to privacy control DM-2, Data Retention and Disposal.

SORN 48VA40B: Retained indefinitely.

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

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner.

This question is related to privacy control DM-2, Data Retention and Disposal.

48VA40B – Veterans (Deceased) Headstone or Marker Records -VA,
https://www.govinfo.gov/content/pkg/FR-2010-10-21/pdf/2010-26490.pdf

MBMS operates under the following System of Record Notice (SORN):

48VA40B Veterans (Deceased) Headstone or Marker Records -VA, per Title 38, United States Code: Sections 501(a), 501(b), and Chapter 24, Sections 2400-2404, which states that records are retained indefinitely, in support of the mission to memorialize Veterans and their family members.
https://www.archives.gov/about/records-schedule
Collections Related to Records Reconstruction
1465
National Personnel Records Center (NPRC) Collection of Military Personnel-Related Records Used in Records Reconstruction

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.?

This question is related to privacy control DM-2, Data Retention and Disposal.

Electronic media sanitization, when the records are authorized for destruction (or upon system decommission), will be carried out in accordance with VA 6500.1 HB Electronic Media Sanitization. Once entered into the electronic system, records in MBMS are stored forever. This includes faxes, which are stored electronically in the Feith document database (the document repository NCA leverages for file storage and reference). This is due to the unique nature of the system's mission to memorialize Veterans.

Program listings and documentation relating to the use of or access to a computer system require special handling if the listings or documentation provide information about a system that processes sensitive data. VA personnel are responsible for retrieving/removing all printed outputs they request from printers. All VA personnel responsible for these activities must complete annual cybersecurity and privacy awareness training.

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

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?

This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

PII collected by MBMS is not used for research, training, or testing.

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

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

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

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

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

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?

This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk: There is a risk that information will be stored in the system for longer than necessary.

Mitigation: MBMS stores data indefinitely as mandated by the following System of Record Notice (SORN):48VA40B – Veterans (Deceased) Headstone or Marker Records -VA, per Title 38, United States Code: Sections 501(a), 501(b), and Chapter 24, Sections 2400-2404, which states that records are retained indefinitely, in support of the mission to memorialize Veterans and their family members.

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***
VBMS E-Folder	Store information once received and process	PII - Veteran Benefit information documentation	Representational State Transfer (REST) Web Service API (HTTP)
Identity and Access Management (IAM)	User access control	PII - Identity Access Information for User access control: Name, Address, SSN (Data Encrypted)	REST Web Service API (HTTP)
Burial Operations Support System - Enterprise (BOSS-E)	To support legacy users	Memorial Information; Birth Date, Email, Name, Gender, Address, Date of Death, Marital Status, Military honors, Relationship to Veteran, SSN, Phone, County, Military Service Release from Active Duty (RAD) Date, Veteran's Period of Service, and Veteran's War Period	Secure Database Connection - Oracle Forms based application backed by an Oracle 12c database

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*
VA Master Persons Index (MPI)-Enterprise (MPIe)	To have the ability to search the authoritative data source for Veterans, MPI, to ensure that they are not creating duplicate contact records in applications built on the Salesforce platform.	First Name, Middle Name, Last Name, Social Security Number (SSN), Date of Birth (DOB), Gender, Phone Number, Place of Birth (POB) City, Place of Birth (POB) State, Mother's Maiden Name	REST Web Service API (HTTP)

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: The privacy risk associated with maintaining SPI is that this data may be disclosed to individuals who do not require access, which would increase the risk of the information being misused.

Mitigation: Safeguards are implemented to ensure data is not sent to unauthorized VA employees, including employee security and privacy training, and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized for the system.

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***
Salesforce	The MBMS application will need to push/pull data from existing NCA data sources via Rest APIs exposed by MBMS.	First Name, Middle Name, Last Name, SSN, Gender, Marital Status, Service Number, Birthdate, Date of Death, Address Line One, Address Line Two, City, State, Zip, Code, County, Country, Birth Sex, Self-Identified Gender, Self-Identified Gender Comment, Home of Record in Service	48VA40B – Veterans (Deceased) Headstone or Marker Record s-VA, per Title 38, United States Code: Sections 501(a),	HTTPS

	Function-ality build includes Case Manage-ment, Eligibility, and Scheduling.	Area, Ethnicity, Race(s), Race Comment, Email	501(b), and Chapter 24, Sections 2400-2404. ISA/MOU between Salesforce and MBMS systems.	
VAEC AWS	AWS hosted in VAEC is the government cloud that will serve as the infra-structure that hosts the BIP platform as a service and subsequent hosted minor application, MBMS.	Personally Identifiable Information (PII): Veteran's and Next-of-Kin's data including Name, SSN, Birthdate, Date of Death, Gender, Marital Status, and Address of Record. Veteran Data to include Name, SSN, Birthdate, Date of Death, Gender, Marital Status, Address of Record, Military Service Number, Military Service Entered on Duty (EOD) Date, Military Service Release from Active Duty (RAD) Date, Veteran's Period of Service, and Veteran's War Period	MBMS is a minor application under the BIP Platform ATO – all VAEC AWS agree-ments are between BIP and VAEC	HTTPS

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

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

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.

Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.

This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing.

Follow the format below:

Privacy Risk: There is a risk that information may be shared with an external organization or agency that does not have a need or legal authority to access VA data.

Mitigation: Only authorized individuals may have access to the data and only when needed to perform their duties. They are required to take the annual VA mandatory data privacy and security training. Authorized Individuals authenticate through Identity and Access Management (IAM) Single Sign-On Internal (SSOi) and User Provisioning for access to the system and data.

According to SORN 48VA40B, "Disclosure of relevant information may be made to individuals, organizations, private or public agencies, or other entities with whom VA has a contract or agreement or where there is a subcontract to perform such services as VA may deem practicable for the purposes of laws administered by the VA, in order for the contractor or subcontractor to perform the services of the contract or agreement."

Section 6. Notice

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

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

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

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

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

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

At the time that the Veteran or NOK call in to request cemetery services, they have already been given a Privacy Act Information and Respondent Burden by the Pre-Need eligibility division, which addresses the collection of information and advises the obligation to respond is voluntary.

- 40-10007, Application for Pre-Need Determination of Eligibility for Burial Form VA Form 40-10007 https://www.cem.va.gov/pre-need/
- 175/VA41A – VA National Cemetery Pre-Need Eligibility Determination – per Title 38, United States Code: Sections 501(a), 501(b), and Chapter 24 Section 2402 https://www.govinfo.gov/content/pkg/FR-2016-08-17/pdf/2016-19591.pdf
- 40-1330, Headstone or Marker Claim for Standard Government Headstone or Marker Form: https://www.va.gov/vaforms/va/pdf/VA40-1330.pdf
- 40-1330M, Medallion Claim for Government Medallion for Replacement in a Private Cemetery Form: https://www.va.gov/vaforms/va/pdf/VA40-1330M.pdf
- 48VA40B – Veterans (Deceased) Headstone or Marker Records -VA, per Title 38, United States Code: Sections 501(a), 501(b), and Chapter 24, Sections 2400-2404 https://www.govinfo.gov/content/pkg/FR-2010-10-21/pdf/2010-26490.pdf

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

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached.

This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.

Responding to collection is voluntary; however, if information is not provided; then benefits may be denied.

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.

Responding to collection is voluntary; therefore, consent of use is not applicable.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

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

Privacy Risk: There is a risk that members of the public may not know that the Memorial Benefits System exists within the Department of Veterans Affairs.

Mitigation: VA mitigates this risk by providing the public with three forms of notice that the system exists; the Privacy Impact Assessment and the System of Record Notice.

- 40-10007, Application for Pre-Need Determination of Eligibility for Burial Form: VA Form 40-10007 https://www.cem.va.gov/pre-need/
- 40-1330, Headstone or Marker Claim for Standard Government Headstone or Marker Form: https://www.va.gov/vaforms/va/pdf/VA40-1330.pdf
- 40-1330M, Medallion Claim for Government Medallion for Replacement in a Private Cemetery Form: https://www.va.gov/vaforms/va/pdf/VA40-1330M.pdf

Section 7. Access, Redress, and Correction

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

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

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

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

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

This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

VHA Handbook 1605.1 Appendix D "Privacy and Release Information", section 7(b) states the rights of the Veterans to request access to review their records. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to and reviewed by the System Manager for the concerned

VHA system of records, the facility Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted.

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.

Requests for records should be submitted as a written request to the Privacy Officer, National Cemetery Administration, Department of Veterans Affairs, 810 Vermont Avenue, NW, Washington, DC 20420. All inquiries should include the individual's full name, branch of service, dates of service, service numbers, social security number, and date of birth.

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

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

This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Individuals are notified of procedures for correcting their information via SORN published in the Federal Register (SORN 48VA40B).

48VA40B – Veterans (Deceased) Headstone or Marker Records-VA.
https://www.govinfo.gov/content/pkg/FR-2010-10-21/pdf/2010-26490.pdf

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.

This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

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

Formal redress procedures are published in the Federal Register per SORN 48VA40B.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?

This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk: There is a risk that the individual accidentally provides incorrect information in their correspondence.

Mitigation: Before entering data into the Legacy BOSS-E components of MBMS, data are manually verified and cross referenced against available information on DD Form 214. Since the information is also submitted directly from an individual, all information may be validated with the original source. The individual may also follow the steps in section 7.2 for correcting information.

Section 8. Technical Access and Security

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

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

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

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

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

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

Following IAM User Provisioning as implemented for MBMS, user roles, such as Cemetery Representative or Cemetery Director, identify the information and application components a user can access. The Cemetery Director has privileges to set and modify the cemetery business rules used to determine scheduling availability. Cemetery Representatives provide operations support at each cemetery. To receive access to MBMS, another system user with appropriate permissions must sponsor them. The sponsor will describe which functionality the user needs to access, the user's role, and any security caveats that apply to the user. These roles will be governed by permission sets that allow field level control of the information and data. MBMS performs Access Control using a Role-Based Access Control (RBAC) model. MBMS uses the Function Roles assigned to a user to make authorization decisions regarding resource access at all layers, which includes the UI, Data, and Services layers. After a user logs in using IAM SSOi, IAM User Provisioning Roles determine the application permissions granted to the user to make authorization decisions.

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.

Booz Allen Hamilton's contractor team supports the MBMS Production environment, and as such, has access to the MBMS system and data contained therein. This includes PII and VA Sensitive Information. The contractors who provide support to the system are required to complete an NDA when onboarding to the MBMS project, in addition to the annual VA Privacy and Information Security and Rules of Behavior training via VA's Talent Management System (TMS). The NDA is kept on file for the duration of the team member's participation on the project. The VA Contracting Officer Representative (COR) for the Booz Allen Hamilton MBMS contract, along with the MBMS System Owner, maintains governing authority over all MBMS environments. The Booz Allen Hamilton MBMS team will maintain users, update applications and components, introduce new functionality, govern deployment activities, and ensure user operability. The Booz Allen Hamilton team members are not primary users of MBMS. The VA COR will monitor and review MBMS related support contracts on a regular basis to ensure there are no gaps in support for the MBMS user community.

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

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately.

This question is related to privacy control AR-5, Privacy Awareness and Training.

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training that all personnel must complete via VA's Talent Management System 2.0 (TMS). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the privacy and security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS 2.0 system.

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

If Yes, provide:

1. *The Security Plan Status,*
2. *The Security Plan Status Date,*
3. *The Authorization Status,*
4. *The Authorization Date,*
5. *The Authorization Termination Date,*
6. *The Risk Review Completion Date,*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

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

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

1. Security Plan Status: Approved
2. Security Plan Status Date: August 22, 2022
3. Authorization Status: Authorization to Operate (ATO)
4. Authorization Date: May 26, 2022 (MBMS), Jan 6, 2022 (BIP – Major Application)
5. Authorization Termination Date: January 6, 2023
6. Risk Review Completion Date: May 26, 2022
7. FIPS 199 classification: Moderate (MBMS), High (BIP – Major Application)

Section 9 – Technology Usage

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

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

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

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

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

MBMS is built as containerized microservices deployed in a Federal Risk and Authorization Management Plan (FEDRAMP)-approved cloud service provider (CSP) environment. Security controls are managed at three levels: FEDRAMP, General Support Services (GSS), and the MBMS application level. FEDRAMP and GSS control details are available in VA Enterprise Cloud (VAEC) Amazon Web Services (AWS) accreditation documentation.

The VAEC provides infrastructure-as-a-service (IaaS), software-as-a-service (SaaS), and platform-as-a-service (PaaS) IT services to VA customers. MBMS is hosted on virtual servers located in the VAEC AWS environment. Using VAEC AWS as the hosting platform for MBMS provides the following operational tools in a FedRAMP-approved environment:

- Self-service catalog
- Provisioning, orchestrating, and deployment
- Access and security management
- Resourcing and account management
- Backup and disaster recovery services

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

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

Contract Number: VA118-16-D-1007

National Cemetery Administration (NCA) will have rights over MBMS data.

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.

The CSP relationship is managed via the Major Application relationship with BIP Assessing. The VAEC AWS maintains the DI-1 control within their boundary.

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.

MBMS leverages the VAEC Cloud Service Provider (CSP) AWS GovCloud, which is FEDRAMP approved, under the BIP Assessing ATO. Per the approval of the Deputy Assistant Secretary, Enterprise Program Management Office (EPMO) [the VA Authorizing Official (AO)], VA Business Stakeholders of the BIP minor applications have ownership rights over data. National Cemetery Administration (NCA) will have rights over MBMS data.

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).

The MBMS System does not utilize Robotics Process Automation (RPA) in any processes.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

Cynthia A. Merritt 297052

Digitally signed by Cynthia A. Merritt 297052
Date: 2022.10.03 09:14:18 -04'00'

Privacy Officer, Cynthia Merritt

JOSEPH FACCIOLLI

Digitally signed by JOSEPH FACCIOLLI
Date: 2022.10.03 11:04:37 -04'00'

Information Systems Security Officer, Joseph Facciolli

MICHAEL OUSLANDER

Digitally signed by MICHAEL OUSLANDER
Date: 2022.10.03 12:17:59 -04'00'

nformation Systems Owner, Michael Ouslander

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).

- SORN 48VA40B – Veterans (Deceased) Headstone or Marker Records -VA
- https://www.govinfo.gov/content/pkg/FR-2010-10-21/pdf/2010-26490.pdf
-
- 40-10007, Application for Pre-Need Determination of Eligibility for Burial Form VA Form 40-10007 https://www.cem.va.gov/pre-need/
-
- 40-1330, Headstone or Marker Claim for Standard Government Headstone or Marker Form: https://www.va.gov/vaforms/va/pdf/VA40-1330.pdf
-
- 40-1330M, Medallion Claim for Government Medallion for Replacement in a Private Cemetery Form: https://www.va.gov/vaforms/va/pdf/VA40-1330M.pdf

- 175/VA41A – VA National Cemetery Pre-Need Eligibility Determination – per Title 38, United States Code: Sections 501(a), 501(b), and Chapter 24 Section 2402 https://www.govinfo.gov/content/pkg/FR-2016-08-17/pdf/2016-19591.pdf