Privacy Impact Assessment for the VA IT System called:

Burial Operations Support System Enterprise AWS

National Cemetery Administration (NCA)

Memorial Benefits and Services

eMASS ID # 1974

Date PIA submitted for review:

07-16-2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Cindy Merritt	Cindy.merritt@va.gov	321-200-7477
Information System Security Officer (ISSO)	Karen McQuaid	Karen.McQuaid@va.gov	708-724-2761
Information System Owner	April Cornelison	April.cornelison@va.gov	512-214-4559

Abstract

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

As authorized under the National Cemeteries Act of 1973, the Memorial Benefits System (MBS) is a system enclave consisting of two major components, Burial Operations Support System/Automated Monument Application System (BOSS and AMAS) and several minor interdependent components that utilize common data to automate all business processes associated with monuments and interments.

Overview

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

1 General Description

A. What is the IT system name and the name of the program office that owns the IT system?

Burial Operations Support System Enterprise AWS. Memorial Benefits and Services.

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

The Memorial Benefits Application (MBS) is a Major Application hosted in the VAEC AWS environment and at the Quantico Information Technology Center (QITC), managed by Infrastructure Operations (IO). The MBS serves customers in the National Cemetery Administration (NCA) and their partners, State/Tribal/Military Cemeteries to provide memorial benefits for Veterans and their families. The Burial Operations Support System (BOSS) was developed to provide benefit delivery automation to support National and State Veteran Cemeteries nationwide and automate the manual, paper-intensive record keeping, information, and forms processing associated with interments. BOSS allows The National Cemetery Administration (NCA) to provide electronic transfer of information for the VA corporate master Veteran identification initiative. The Automated Monument Application System (AMAS) was developed to provide the required automation of all business processes associated with monument applications (e.g., ordering, delivering, and tracking). Through ongoing development of the automation, integration, and standardization of AMAS functions, NCA can accommodate an increasing workload; maximize the utilization of personnel and physical resources, and capture information needed for Memorial Program Service (MPS) and VA information resources management planning activities. The VA required nationwide burial location capabilities; and the ability to link gravesite reservation files and provide a benefit cross-check facility for timely First Notice of Death (FNOD) to Veterans Benefits Administration (VBA).

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

National Cemetery Administration (NCA).

2. Information Collection and Sharing

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

BOSS processes approximately 150,000 burial cases per year. AMAS processes approximately 360,000 applications (via VA Form 1330) for government-furnished monuments each year; including headstones, markers, medallions, and niche covers. AMAS tracking capability expedites claims research and NCA's subsequent response to case inquiries. The system processes PII data for Veterans or their dependents as well as members of the public/individuals. The list of data elements collected, used, disseminated, created, or maintained in the system can be seen in section 1.1 below.

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

BOSS-E AWS is a system of systems consisting of 10 VA legacy sub-systems: Burial Operations Support System (BOSS), Automated Monument Application System (AMAS), Eligibility Office Automation System (EOAS), Nationwide Gravesite Locator (NGL), Presidential Memorial Certification (PMC), Daily Burial Schedule (DBS), Kiosk - Nationwide Gravesite Locator (KGL), Memorials Enterprise Fax System (MEFS), Gravesite Assessment Reporting (GAR), Management, Memorials Administration Decision Support System (MADSS). The Burial Operations Support System (BOSS) was developed to provide benefit delivery automation to support National and State Veteran Cemeteries nationwide and automate the manual, paper-intensive record keeping, information, and forms processing associated with interments. BOSS allows the National Cemetery Administration (NCA) to provide electronic transfer of information for the VA corporate master Veteran identification initiative. BOSS processes approximately 150,000 burial cases per year. The VA required nationwide burial location capabilities; and the ability to link gravesite reservation files and provide a benefit cross-check facility for timely First Notice of Death (FNOD) to Veterans Benefits Administration (VBA). The Automated Monument Application System (AMAS) was developed to provide the required automation of all business processes associated with monument applications (e.g., ordering, delivering, and tracking). Through ongoing development of the automation, integration, and standardization of AMAS functions, NCA can accommodate an increasing workload; maximize the utilization of personnel and physical resources; and capture information needed for Memorial Program Service (MPS) and VA information resources management planning activities. AMAS processes approximately 360,000 applications for government-furnished monuments each year: including headstones, markers, and niche covers. AMAS tracking capability speeds up claims research and the NCA's subsequent response to case inquiries.

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

BOSS-E AWS shares information with other internal VA organizations but does not share any data/information with external organizations.

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

The BOSS-E AWS alpha, beta, pre-test, and production environments are hosted in the VAEC in AWS GovCloud. Feith and MEFS are hosted at QITC. There is no other site it operates from.

3. Legal Authority and SORN

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

48VA40B - Veterans (Deceased) Headstone or Marker Records - VA.
AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 38 U.S.C. 2404.

I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?

No, the SORN does not cover cloud usage or storage.

4. System Changes

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

NO

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

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

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

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

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

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

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☒ Personal Fax Number
- ☒ Personal Email Address
- ☒ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers[1]
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☐ Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☒ Gender
- ☐ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☒ Next of Kin
- ☒ Other Data Elements (list below)

Other PII/PHI data elements: Date of death, Gender Code, Relationship Code, Veteran ID, Spouse name, Descendent Name, Cemetery, Country, Monument ID, Monument type and Description, Case status, Discharge Type, Service number, War award, branch, rank, date entered on duty, date released from active duty, date case established, home of record, Next of Kin (NOK) information/address.

PII Mapping of Components (Servers/Database)

Burial Operations Support Systems Enterprise (BOSS E) Amazon Web Services (AWS) consists of 2 key components (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Burial Operations Support Systems Enterprise (BOSS E) Amazon Web Services (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.

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

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
BOSS	YES	YES	• Name • Personal Mailing Address • Email Address • Emergency Contact Information • Social Security Number (SSN) • Date of Birth • Personal Phone Number(s) • Personal Fax number • Emergency Contact Info (Name, Phone Number, etc. of a different individual) • Date of Death • Gender Code • Relationship Code • Veteran ID • Descendent name • veteran ID • spouse name • cemetery • country • monument ID • Monument Type and Description • Case status • discharge type • service number	Memorial benefit delivery automation support	Database encryption and access control

			• monument type and description • war award • date of death • branch • rank • date entered on duty • date released from active duty • date case established • Home of record • Next of Kin |NOK| information/address		
Automated Monument Application System AMAS	YES	YES	• Name • Personal Mailing Address • Email Address • Emergency Contact Information • Social Security Number (SSN) • Date of Birth • Personal Phone Number(s) • Personal Fax number • Emergency Contact Info (Name, Phone Number, etc. of a different individual) • Date of Death • Gender Code • Relationship Code • Veteran ID • Descendent name • veteran ID • spouse name • cemetery • country • monument ID • Monument Type and Description • Case status • discharge type	Processing application for monument (burial headstones)	Database encryption and access control

			• service number • monument type and description • war award • date of death • branch • rank • date entered on duty • date released from active duty • date case established • Home of record • Next of Kin |NOK| information/address		

1.2 What are the sources of the information in the system?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

The Memorial Benefits System (MBS)-BOSS component receives data from funeral homes, next of kin, and other points of contact for the decedent for burial services. The AMAS component collects data directly from individuals as part of a monument application.

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.

Given the purpose of the Memorial Benefits System, the individuals for which the data is being collected are decedent Veterans or their deceased family members, so the information will always need to be collected on their behalf.

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

This system receives data from other sources. It does not create its own information.

1.3 How is the information collected?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from

another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?
BOSS-E AWS does not receive information electronically from other systems. A long-term plan is in place for the Pre-Need system to transmit data electronically to the EOAS component of BOSS, but these activities are currently processed by scheduling office personnel. Documents from funeral homes, next of kin, and other points of contact from the decedent are sent to scheduling office personnel and uploaded into BOSS-E.

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?
Data from the forms are manually entered into the system. Forms and supporting documentation required to verify memorial benefits eligibility, such as the DD214, are scanned/uploaded.
PRESIDENTIAL MEMORIAL CERTIFICATE REQUEST FORM OMB Control Number 2900-0567.

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

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

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.
Data is manually verified by the Scheduling Office through Beneficiary Information Record Locator System (BIRLS) for accuracy. The information stored in the system is checked for accuracy by cross-referencing the data with information available on DoD Forms 214 or other sources (e.g., data received from previous benefit requests). Additionally, since the information is submitted directly from an individual, the information may be validated with the original source.

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?
BOSS-E AWS does not check for accuracy by accessing a commercial aggregator of information.

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect

BOSS-E AWS 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.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: BOSS/AMAS collects the SPI on deceased Veterans and limited contact information from their next of kin/point of contact for arranging the burial. If this information were 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, 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.
VA applies consistent security guidance to centralize and standardize account management, network access control, database security, vulnerability scanning, and remediation. NCA Information Security Officer is responsible for administering 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 that will be used in support of the program's business purpose.

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

PII/PHI Data Element	Internal Use	External Use
Name	File Identification purposes. To verify Veteran or decedent's identification	Also collected if subject is a contact person for decedent.
Social Security Number	Used to verify Veteran or subject's identity.	
Spouse Name	Obtained as needed for monument inscription or as Next of Kin	
Date of Birth	Needed for monument inscription.	
Mailing Address	Collected for decedent's POC.	Collected for decedent's POC.
Phone Number	Collected for decedent's POC.	Collected for decedent's POC.
Fax Number	Collected for decedent's POC.	Collected for decedent's POC.
Email Address	Collected for decedent's POC.	Collected for decedent's POC.
Emergency Contact	Just the POC (not emergency).	Just the POC (not emergency).
Service Information: e.g., Service number, branch, rank, date entered on duty, date released from active duty, date case established.	Used to verify Veteran's eligibility.	
Benefit Information	Used to verify burial benefits.	Used to verify burial benefits.
Relationship to Veteran	Required when the decedent is not the Veteran to determine eligibility.	Required when the decedent is not the Veteran to determine eligibility.
Date of Death	Needed for monument inscription.	
Gender Code	Used to identify prefix to communicate (Mr./Mrs./Ms.)	
Relationship Code	Define relationship to Veteran.	Define relationship to Veteran.
Veteran ID	Used to link the individual to the Veteran file.	Used to link the individual to the Veteran file.
Cemetery	Identify where decedent is interred.	Identify where decedent is interred.
Country	To determine the Veterans or decedent's country of origin.	

Monument ID	Unique ID for the monument	
Monument Type and Description	Defines the type of monument	
Case status	Used to show status of case.	
Discharge type	Used to determine eligibility.	
War award	Used to determine eligibility.	
Home of record	Used to determine distance from preferred cemetery.	
NOK information/address	Identifies POC	Identifies POC

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis?
The BOSS-E AWS system itself does not perform any kind of analysis or run analytic tasks in the background.

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.
The BOSS-E AWS system itself does not perform any kind of analysis or run analytic tasks in the background.

2.3 How is the information in the system secured?
These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

2.3a What measures are in place to protect data in transit and at rest?
Information is protected at rest through AES-256 encryption using AWS KMS secure server side, when stored in Oracle RDS and S3 buckets. Information is protected in transit through TLS 1.2 with an AES-256 cipher. The Oracle RDS database is in a private subnet, protected by an AWS Security Group that allows access only from application servers and a bastion host in the same AWS VPC. So, it is not possible to connect directly to the database from outside the VPC.

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

Access to SSNs is limited to those with a need-to-know via database authentication and role-based grants. SSNs are removed from communications and copies of data.

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?
Per the SORN, NCA will maintain the data in compliance with applicable VA security policy Directives that specify the standards that will be applied to protect sensitive personal information. Further, only authorized individuals may have access to the data and only when needed to perform their duties. They are required to take annual VA mandatory data privacy and security training. The system ensures that through the implementation of the Risk Management process, appropriate administrative, technical and physical controls/safeguards have been allocated and documented in the GRC tool(eMASS) to protect the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained.

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?

Authorized users of BOSS-E AWS information systems are those who have completed:
•A background screening,
•VA Privacy and Information Security Awareness and Rules of Behavior training,
•Approved access request (9957 form or YourIT Memorials Application Account Request)

VA employees/contractors use ePASS and require approvals from supervisors.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented?
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 the MBS application cover 18 security areas related to protection of the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security areas include access control; awareness and training; audit and accountability; assessment,

accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. The MBS application team has implemented the required security controls based on the tailoring guidance of NIST Special Publication 800-53 Rev 4 and VA directives or handbooks.

2.4c Does access require manager approval?

NCA management designates Account Managers for the management of information system accounts. Only OIT staff are authorized to create, enable, modify, disable, and remove information system accounts upon receipt of an access request form approved by the appropriate individuals.

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

Yes. 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. Records are maintained on paper and are stored at VA Central Office.

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

The BOSS-E AWS Information System Owner is responsible for assuring safeguards for the PIIA. The application team has implemented the required security controls based on the tailoring guidance of NIST Special Publication 800-53 Rev 4 and VA directives or 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

•Name• Personal Mailing Address• Email Address• Emergency Contact Information• Social Security Number (SSN)• Date of Birth• Personal Phone Number(s)• Personal Fax number• Emergency Contact Info (Name, Phone Number, etc. of a different individual) • Date of Death• Gender Code• Relationship Code• Veteran ID• Descendent name• veteran ID• spouse name• cemetery• country• monument ID •Monument Type and Description• Case status• discharge type• service number• monument type and description• war award• date of death• branch• rank• date entered on duty• date released from active duty •date case established• Home of record • Next of Kin(NOK) information/address.

3.2 How long is information retained?

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

According to the SORN 48VA40B, records in this system are retained permanently in accordance with the schedule approved by the Archivist of the United States, NCA Records Control Schedule, NC1–15–85–9 item 21g(1)(a).

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner. Please work with the system Privacy Officer and VA Records Officer to answer these questions.
This question is related to privacy control DM-2, Data Retention and Disposal.

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

Yes. The retention schedule has been approved by the VA records office and NARA. The retention schedule 1180.17 for Veterans Benefits indicates to "Cutoff after receipt of last relevant correspondence. Transfer to NARA 50 years after cutoff."
https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf

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

48VA40B - Veterans (Deceased) Headstone or Marker Records. The retention schedule 1180.17 for Veterans Benefits indicates to "Cutoff after receipt of last relevant correspondence. Transfer to NARA 50 years after cutoff." Disposition Authority N1-15-06-2, item 18.

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.

Paper records are destroyed upon manual entry into the MBS; this is an NCA business process external to the MBS system. 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 the MBS

are stored forever. This includes faxes, which are stored electronically in the Feith document database. This is due to the unique nature of the system's mission to memorialize Veterans. Forms and other types of printed output produced by any computer systems and related peripherals will be evaluated by the responsible staff member for data sensitivity. Printed output containing sensitive data will be stored in locked cabinets or desks and disposed of properly (when the approved records schedule 6371. 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. permits destruction) by shredding or similar VA-approved methods in accordance with VA Directive.

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.
PII collected by BOSS-E AWS is not used for research, testing or training.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

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

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

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

Follow the format below:

Privacy Risk: 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 (SPl) 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.

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***
AITC - Master Person Index (VA MPI) via VA Authentication Federation Infrastructure (VAAFI)	Verifies and updates MEL record when Updated in the MBS (BOSS/AMAS)	Date of Birth, Date of Death, Gender Code, Veteran ID, Relationship Code, Name, Social Security Number	Encrypted using a web service from server (MBSQITC) to server (MPIAITC): sent to A database queue by Oracle triggers; MVI (web service program) picks up the data from the database queue.
Memorial Enterprise Letters (MEL)	MEL pulls the Veteran case data from AMAS to generate a new letter, also updates AMAS with the completed letter and letter status.	Decedent Name, Veteran ID, Spouse Name, Cemetery, Country, SSN, Monument ID, Case Status, Discharge Type, Service Number, Monument Type and Description, War Awards, Date of Birth, Date of Death, Branch, Rank, Date Entered on Duty, Date Released from Active Duty, Date Case Established.	Java Database Connectivity (JDBC)
Secure File Transfer Protocol (SFTP) Server - Accessed by NCA users with approved access authorizations (VA Form 9957) on file; NCA users log in/download the file as needed to update the GovDelivery email list of funeral home contacts.	A cron job called "ncso-listbuilder" extracts BOSS funeral home contact e-mail addresses and posts the output report to the SFTP Server for approved users to access for NCA authorized business purposes.	Email addresses for funeral home points of contact.	SFTP comma-separated values (CSV) file

Memorial Benefits Management System (MBMS)	Provide a replacement for the Burial Operations Support System Enterprise (BOSS-E) by replacing BOSS-E's sub-applications with a more cohesive enterprise system while incorporating new functionality and process improvement. Implemented through a series of successive builds that will provide continuous improvements in functionality while moving users off the legacy systems and culminate with BOSS-E's decommissioning. Provides an increase in benefits delivery efficiency to Veterans and their families by improving access to benefits tracking and delivery, enhancing end-user functionality to the system, and providing increased customer service satisfaction through shorter processing times. Connection is required between BOSS and the MBMS to support the entire memorials case lifecycle: Time of need cases will be established in the MBMS leveraging legacy data in BOSS for case validation. Once the case manager has conducted eligibility and completed scheduling of the internment, the case will be transferred to the BOSS system for	Veteran ID, Decedent or Veteran Name, SSN, Date of Death, Date of Birth, Gender Code, Relationship Code, home of record, spouse name, cemetery, country, case status, discharge type, service number, war awards, service number, branch, rank, date entered on duty, date released from active, Next of Kin(NOK) information/address, monument ID, monument type and description, spouse information, email addresses for funeral home points of contact.	Direct database connection from the MBMS to BOSS/AMAS.

	downstream processing and reporting.		

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: 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: The principle of need-to-know is strictly adhered to by the MBS (BOSS/AMAS) personnel. Only personnel with a clear business purpose are allowed access to the system and to the information contained within.

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***
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: Not applicable, as there is no sharing of information outside of NCA or VA with external agencies.

Mitigation: Not applicable, as there is no sharing of information outside of NCA or VA with external

Section 6. Notice

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

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

Individuals are notified of collection information via the SORN published in the Federal Register (48VA40B) and via the respondent burden cited on relevant forms. BOSS-E AWS operates under the following System of Record Notice (SORN):48VA40B - Veterans (Deceased) Headstone or Marker Records.

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

A notice is provided and below are the links to the various forms.

•40-0247, PMC Presidential Memorial Certificate Request
Form: https://vaww.va.gov/vaforms/va/pdf/VA40-0247.pdf

•40-1330, Headstone or Marker Claim for Standard Government Headstone or Marker form:
HTTPs://vaww.va.gov/vaforms/va/pdf/VA40-1330.pdf

•40-1330M, Medallion Claim for Government Medallion for Replacement in a Private Cemetery Form:
https://vaww.va.gov/vaforms/va/pdf/VA40-1330M.pdf

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

https://vaww.va.gov/vaforms/va/pdf/VA40-0247.pdf. A statement at the top page of the Presidential Memorial Certificate Request Form reads “The National Cemetery Administration does not give, sell, or transfer any personal information outside of the agency. The Department of Veterans Affairs (VA) may not conduct or sponsor, and you are not required to respond to this collection of information unless it

displays a valid OMB Control Number. Responding to this collection is voluntary. Send comments regarding this burden estimate or any other aspects of this collection of information, including suggestions for reducing this burden, to VA Clearance Officer (005R1B), 810 Vermont Avenue NW, Washington, DC 20420. SEND COMMENTS ONLY. Please do not send applications for benefits to this address."

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

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

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

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

Privacy Risk: There is a risk that members of the public may not know that the Memorial Benefits System exists within the VA.
Mitigation: VA mitigates this risk by providing the public with two forms of notice that the system exists; the Privacy Impact Assessment and the System of Record Notice.

Section 7. Access, Redress, and Correction

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

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

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

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

Individuals seeking information on the existence and content of records in this system pertaining to them should contact the system manager in writing as indicated above. A request for access to records must contain the requester's full name, address, telephone number, be signed by the requester, and describe the records sought in sufficient detail to enable VA personnel to locate them with a reasonable amount of effort. Information collected in BOSS/AMAS can be accessed under the FOIA and Privacy Act regulations; Title 5, U.S. Code subsection 552 and Title 5, U.S. Code subsection 552a. Records can be requested electronically at ncafoia@va.gov or contacting NCA FOIA Officer, Nikki Benns, at Nikki.Benns@va.gov.

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)?
BOSS-E AWS is not exempt from the access provisions of the Privacy Act.

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information?
BOSS-E AWS is a Privacy Act System. Individuals seeking information on the existence and content of records in this system pertaining to them should contact the system manager in writing as indicated above. A request for access to records must contain the requester's full name, address, telephone number, be signed by the requester, and describe the records sought in sufficient detail to enable VA personnel to locate them with a reasonable amount of effort.

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

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

Individuals seeking to contest or amend records in this system pertaining to them should contact the system manager in writing as indicated above. 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. Requests for records can be submitted electronically at ncafoia@va.gov or by contacting NCA FOIA Officer, Nikki Benns, at Nikki.Benns@va.gov.

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).

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.
Individuals are notified of procedures for correcting their information via SORN published in the Federal Register (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.*** *(Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

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

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

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

Follow the format below:

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

Mitigation: Before entering data into the BOSS/AMAS components of MBS, data are manually verified and cross referenced against available information on DoD Form 214. Since the information is submitted directly from an individual, the information may be validated with the original source. Section 8. Technical Access and Security.

Section 8. Technical Access and Security

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

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

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system?

NCA will maintain the data in compliance with applicable VA security policy Directives that specify the standards that will be applied to protect sensitive personal information. Further, only authorized individuals may have access to the data and only when needed to perform their duties. They are required to take annual VA mandatory data privacy and security training.

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?

NCA follows Access Control policy as prescribed for VA Enterprise in VA Directive and Handbook 6500. Only VA personnel may access VA-owned equipment used to process VA information or access VA processing services. Employees and contractors may not share with non-VA employees or unauthorized personnel instruction or information regarding how to establish connections with VA private networks and computers. Personnel may not share remote access logon IDs, passwords, or other authentication means used specifically to protect VA information or access techniques to VA private networks.

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.
VA information systems utilize Group Policy Objects (GPO) to manage Active Directory accounts. GPOs consist of a set of rules which control the working environment of user accounts and computer accounts. The GPOs provide the centralized management and configuration of operating Systems, applications, and users' settings in an Active Directory environment. The GPO restricts certain actions that may pose potential security risks. User accounts are reviewed on a quarterly basis and disabled after 90 days of inactivity. User account requests are approved

by the user's supervisor or the contracting officer technical representative (COTR). General user and administrative Windows accounts are managed through Active Directory.

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.

Yes, VA contractors can have access to BOSS/AMAS. VA contract employee access is verified through authorized VA personnel before access is granted to any contractor. Contracts and contractor access are reviewed annually. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via TMS. 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.

8.3 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.

Yes, VA contractors can have access to BOSS/AMAS. VA contract employee access is verified through authorized VA personnel before access is granted to any contractor. Contracts and contractor access are reviewed annually. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via TMS. 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.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 07-June-2024
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* 10-March-2024
5. *The Authorization Termination Date:* 06-September-2024
6. *The Risk Review Completion Date:* 08-March-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.***
N/A

Section 9 – Technology Usage

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

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?
If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.
Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

Yes. The System is being hosted in VAEC AWS cloud environment and operates both as Infrastructure as a Service (IaaS) and Software as a Service (SaaS).

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?
Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also

involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.
This question is related to privacy control DI-1, Data Quality.

9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?
What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.
Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

CYNTHIA MERRITT

Digitally signed by CYNTHIA MERRITT
Date: 2024.08.06 15:32:32 -04'00'

Privacy Officer, Cindy Merritt

KAREN MCQUAID

Digitally signed by KAREN MCQUAID
Date: 2024.08.07 08:15:20 -05'00'

Information System Security Officer, Karen McQuaid

APRIL CORNELISON

Digitally signed by APRIL CORNELISON
Date: 2024.08.07 10:54:05 -05'00'

Information System Owner, April Cornelison

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).

2023-09838.pdf (govinfo.gov) - 48VA40B - Veterans (Deceased) Headstone or Marker Records -VA.

https://vaww.va.gov/vaforms/va/pdf/VA40-0247.pdf

https://vaww.va.gov/vaforms/va/pdf/VA40-1330.pdf

https://vaww.va.gov/vaforms/va/pdf/VA40-1330M.pdf

HELPFUL LINKS:

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

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

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

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

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