SPLASH PAGE LANGUAGE

The completion of Veterans Affairs Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, system, or practice that collects or uses PII under the authority of the E-government Act of 2002 (44 U.S.C. § 208(b)) and VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment.

The PIA is designed to identify risk associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phases of the System Development Life Cycle (SDLC) of IT systems. It also ensures that privacy protections are built into an IT system during its development cycle. By regularly assessing privacy concerns during the development process, VA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements
under the Federal Information Security Management Act (FISMA).

VA HANDBOOK 6508.1: "Implementation of Privacy Threshold Analysis and Privacy Impact Assessment," July 2015, https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=810&FType=2

Please note that the E-government Act of 2002 requires that a PIA be made available to the public. In order to comply with this requirement PIA will be published online for the general public to view. When completing this document please use simple, straight-forward language, avoid overly technical terminology, and write out acronyms the first time you use them to ensure that the document can be read and understood by the general public.

Privacy Impact Assessment for the VA IT System called:

Appeals RMS Assessing (ARMS)

Veteran Centered Experience (VCE) Unified Digital Experience (UDE)

Date PIA submitted for review:

09/09/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Kary Charlebois	Kary.Charlebois@va.gov	202-382-2906
Information System Security Officer (ISSO)	Pamela Crockett-Williams	Pamela.Crockett-Williams@va.gov	(202) 382-2341
Information System Owner	Eric Hickam	Eric.Hickam@va.gov	512-375-2520

Abstract

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

The Appeals Resource Management System (ARMS) is a relational database and associated web application that will enable the Board to expertly manage and accurately report employee and resource data, both daily and strategically. It will also improve the Board's ability to deliver seamless and integrated support services across the enterprise replacing the manual manipulation of data using multiple spreadsheets with a repository of data that can be more easily manipulated across work products.

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?*

ARMS is under the Appeals Modernization Program, which is a web-based system, hosted in Amazon Web Services (AWS) Gov Cloud, utilizing Amazon Relational Database Service (Amazon RDS) for Oracle, that allows the board to pull ad-hoc reports and combines data from different sources to visualize and develop strategies for the organization as well as workforce planning needs. The purpose of the system is to collect Board of Veterans' Appeals HR data for approximately 10,000 Employees and Applicants from HR SMART/PAID and allow for the manual entry of Appeals HR Data in the ARMS database. ARMS is only accessible internally and will only be shared internally. Currently data is maintained offline across multiple spreadsheets that are manually updated and over time have diverging datasets, injecting errors into reports.

ARMS is a system consisting of a web-based application utilizing Ruby on Rails framework on a Virtual Machine (VM) running Linux and Amazon RDS for Oracle residing in the AWS Gov Cloud. All data is owned by the VA. ARMS has various levels of internal security to control update capabilities to various tables and columns within the ARMS database. Oracle roles have been defined to control update access on a table level. Program logic controls update capability for columns within the database validating both data format integrity and data entry compliance with established business rules and logic. ARMS is currently working on receiving their ATO. ARMS will use the VACOLS SORN as it will be replacing some VACOLS functionality.

Legal authority to operate:

- Veterans' Benefits - Rules and Regulations (Title 38 of the United States Code, Sections 501(a))
- The Privacy Act of 1974, 5 U.S.C. § 552a
- Electronic Code of Federal Regulations (e-CFR), 38 CFR 1.575-1.582
- Recognition of agents and attorneys generally, 38 U.S. Code § 5904
- 44VA01 SORN https://www.govinfo.gov/content/pkg/FR-2013-11-06/pdf/2013-26522.pdf

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)

PII Mapping of Components

ARMS consists of 3 key components (Database Service). Each component has been analyzed to determine if any elements of that component collect Personally Identifiable Information (PII). The type of PII collected by ARMS 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.

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
Database 1	Yes	Yes	SSN - Last 6 digits Name Date of Birth Personal Mailing Address Personal Phone Numbers Personal Email Address Certificate/License numbers	Identification purpose; used to contact individual; Used to manage Bar Accreditation;	SORN Attached
Database 2	Yes	Yes	First name Last name Birth Date, SSN, Veteran Address, Veteran Appeal Information, Veteran Claim Information, Veteran Health Information	Replicated data from CASEFLOW and ARMS used for reporting purposes by the Board of Veterans Appeals	ARMS data at rest resides in volumes utilizing EBS encryption. TLS is utilized for the transfer of data.
Database 3	Yes	Yes	First name Last name Birth Date, SSN, Veteran Address, Veteran Appeal Information, Veteran Claim Information, Veteran Health Information	Replicated data from CASEFLOW and ARMS used for reporting purposes by the Board of Veterans Appeals	ARMS data at rest resides in volumes utilizing EBS encryption. TLS is utilized for the transfer of data.

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.

ARMS collects data from HR tables in Veteran Appeals Control and Locator System (VACOLS). Additionally, users can enter data directly into the ARMS web application.

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.

Data is collected for VACOLS via the Amazon Database Migration service or users directly enter data into the ARMS web application.

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.

The information is provided by the Board Members. The only check for accuracy would be the Board Members reviewing the content of the information provided. The system does not have any technical means for checking for data accuracy.

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

- Veterans' Benefits - Rules and Regulations (Title 38 of the United States Code, Sections 501(a))
- The Privacy Act of 1974, 5 U.S.C. § 552a
- Electronic Code of Federal Regulations (e-CFR), 38 CFR 1.575-1.582
- Recognition of agents and attorneys generally, 38 U.S. Code § 5904
- 44VA01 SORN https://www.govinfo.gov/content/pkg/FR-2013-11-06/pdf/2013-26522.pdf

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: ARMS maintains PII and Personal Health Information (PHI) in order to carry out the mission of processing appeals for VA benefits. If this information were to be compromised or released to inappropriate parties or the public, there could be significant financial, personal, and/or emotional harm to the individuals whose information is contained within the ARMS system.

Mitigation: The Department of Veterans Affairs (VA) ARMS team is careful to only collect the information necessary to carry out the mission of processing appeals for veterans' benefits. By only collecting the minimum PII and PHI needed to process appeals for veterans the risk to veterans is also minimized in the event of a data breach.

Section 2. Uses of the Information

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

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

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

The purpose of the system is to collect Board of Veterans' Appeals HR data for Employees and Applicants from HR SMART/PAID and allow for the manual entry of Appeals HR Data in the RMS database. Currently data is maintained offline across multiple spreadsheets that are manually updated and over time have diverging datasets injecting errors into reports. Once all the data is in the ARMS database it will be easily manipulated across the Board of Veterans' Appeals.

List of PII collected:
Name: used as an identifier
Social Security Number: used as an identifier
Date of Birth: used as an identifier
Personal Mailing Address: used to contact individual
Personal Phone Number(s): used to contact individual
Personal Email Address: used to contact individual
Certificate/License numbers: used to manage Bar Accreditation

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

All data contained within ARMS is analyzed and used only within ARMS. No external program is used to analyze the data.

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?

ARMS data at rest resides in volumes utilizing EBS encryption. TLS is utilized for the transfer of data.

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

ARMS systems are storing Social Security numbers. The ARMS application resides in a secure VA GovCloud enclave that limits connectivity to those connecting from VA equipment, via VA single sign on. All data at rest resides in encrypted volumes and connectivity to the application occurs via TLS/SSL.

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

ARMS users attend VA security training. ARMS data resides in volumes utilizing EBS encryption. TLS is utilized for the transfer of data. Access is limited to users using VA single sign on using VA equipment.

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

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

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

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

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

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.

All VA employees and contractors are required to go through privacy, information security and VA Rules of Behavior (ROB) training. This training ensures that the end users of ARMS know how to properly handle PII. Beyond the training the system is designed to secure the data to ensure that users must be granted access to the system in order to view, modify, add or remove data. System access is limited and controlled by the Board.

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

All information from 1.1 is retained.
Name: used as an identifier
Social Security Number: used as an identifier
Date of Birth: used as an identifier
Personal Mailing Address: used to contact individual
Personal Phone Number(s): used to contact individual
Personal Email Address: used to contact individual
Certificate/License numbers: used to manage Bar Accreditation

3.2 How long is information retained?

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

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

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

Records are retained indefinitely and in accordance with records retention standards approved by the Archivist of the United States, the National Archives and Records Administration, and published in Agency Records Control Schedules. The retention schedules are documented in the SORN.

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.

ARMS falls under Records Control Schedule (RCS) 005-1
https://www.govinfo.gov/content/pkg/FR-2013-11-06/pdf/2013-26522.pdf

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

Elimination of electronic data is inherited from the Veteran Administration Enterprise Cloud (VAEC) AWS. All hardware is housed in the VAEC AWS where the ARMS application and databases reside. All records are retained indefinitely.

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

System access is controlled via Role Based Access Control (RBAC) in order to minimize the risk to privacy of using Personally Identifiable Information (PII) for research, testing or training. Dummy

Data is used for testing and training. Users will be required to use their Personal Identity Verification (PIV) to login to the ARMS application where two factor authentication (2FA) is enabled. Access is granted by the ARMS application team to those users that are approved for access and meet business need requirements. There is a rolling 35 day set of backups maintained in VA GOV Cloud.

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.

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 may be stored for longer than necessary.

Mitigation: There is a rolling 35 day set of backups maintained in VA GOV Cloud. ARMS follows the Records Control Schedule (RCS) 005-1. All information is retained indefinitely.

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***
Board of Veterans Appeals - VACOLS	Migration of data to ARMS for VACOLS Decommissioning. Legacy Appeal information for Board of Veterans Appeals reporting purposes.	PII Name Social Security Number Date of Birth Personal Mailing Address Personal Phone Number(s) Personal Email Address Certificate/License numbers	Electronically, over Secure File Transfer Protocol (SFTP).
Board of Veterans Appeals - CASEFLOW	Veteran Appeal information for reporting purposes.	*PII:* First name Last name Birth Date, SSN, Veteran Address, Veteran Appeal Information, Veteran Claim Information, Veteran Health Information	All traffic subject to TIC (encrypted)

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***
Board of Veterans Appeals - Redshift	Veteran Legacy and AM appeal information data warehouse	First name Last name Birth Date, SSN, Veteran Address, Veteran Appeal Information, Veteran Claim Information, Veteran Health Information	All traffic subject to TIC (encrypted) ; Encrypted Storage
AWS Govcloud	Hosting Service Appeals RMS Application	*PII:* • *Last name* • *First name* • *SSN (employees only)* • *Date of Birth (employees only)* • *Place of Birth (employees only)* • *Address* • *Email* • *Phone number* • *Emergency Contact (employees only)*	All traffic subject to TIC (encrypted) ; Encrypted Storage

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

Follow the format below:
Privacy Risk: There is a risk that information may be accessed by unauthorized organizations or individuals.

Mitigation: The privacy risk to the ARMS information is minimized through various layers of security boundaries. ARMS resides in the secured VA AWS which has FIPS 140-2 encryption enabled. VA AWS practices continuous monitoring through various tools and the overall environment is monitored by CSOC.

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***

ARMS does not share or disclose information externally.

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:
Privacy Risk: ARMS does not share or disclose information externally.

Mitigation: ARMS does not share or disclose information externally.

Section 6. Notice

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

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an appendix. (A 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.

ARMS is replacing VACOLS, and it has an up to date SORN posted on the Federal Register. A Privacy Act Statement is provided on any forms that collect information from individuals. The log on screen will also have the following message:

"You are accessing a U.S. Government information system, which includes:
(1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only. Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties. By using this information system, you understand and consent to the following:
You have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system. At any time, the government may for any lawful government purpose monitor, intercept, search and seize any communication or data transiting or stored on this information system. Any communications or data transiting or stored on this information system may be disclosed or used for any lawful government purpose."

•44VA01 SORN https://www.govinfo.gov/content/pkg/FR-2013-11-06/pdf/2013-26522.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

Employees have the opportunity and right to decline to provide information. In the event that any information is not provided, it may delay processing an employee's future requests for service related to the missing data.

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

Employees have the opportunity and right to decline to provide information. In the event that any information is not provided, it may delay processing an employee's future requests for service related to the missing data. If an employee provides information, they do not have any additional consent on

the use of their information.

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: The individual might be unaware that their information is being collected by the system.

Mitigation: The individual providing information to be used for an appeal is provided with the Privacy Act Notice and the SORN is available for review. This provides the individual with ample notice as to what information is being collected and for what reason.

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.

Access to and use of national administrative database are limited to people whose official duties require such access, and the VA has established security procedures to ensure that access is appropriately limited. Information security officers and system data stewards review and authorize data access requests. VA provides information security training via the Talent Management System (TMS) to all staff and instructs staff on the responsibility each person has for safeguarding data confidentially. Members of the public are not allowed to access ARMS. Employees would have to contact local HR to review their information.

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 can be submitted to the VA using existing VA procedures that conform to the Privacy Act. For example, an employee can contact local human resources liaisons to request a correction. After the information is received by the local human resources liaison, the update is performed manually by VA employees who manage the ARMS data. Employees would have to contact local HR to review or update their information.

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 not notified if there is missing or inaccurate information in their record. An individual who wishes to determine whether a record is being maintained under his or her name in ARMS or wishes to determine the contents of their records should contact their local human resources liaison.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and

Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

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

Employees would have to contact local HR to review or update their information.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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: The individual could accidentally provide incorrect information in their correspondence.

Mitigation: Individuals provide information directly to VA staff or contractors. Any validation performed would merely be the individual personally reviewing the information before they provide it. Individuals are allowed to provide updated information for their records by submitting new forms or correspondence while indicating to the VA that new information supersedes the previous data.

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.

System access is limited and controlled by the Board. The Office of Information and Technology (OIT) also documents and monitors individual information system security training activities including basic security awareness training and specific information system security training. This documentation and monitoring are performed through the use of the Talent Management System (TMS). ARMS will be using Two Factor authentication to allow users internal to VA access to the system using PIV/PIN. Server level access is granted to developers on an as needed basis by the ARMS Information Security Officer (ISO). The ARMS ISO has granted server access to a small set of trusted developers approved to work with and diagnose environment issues. Remote Desktop Protocol (RDP) and Secure Shell (SSH) access is logged and monitored.

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.

Contractors who provide support to the system are required to complete annual training covering VA Privacy, Non-Disclosure Agreement (NDA) and Information Security and Rules of Behavior training via the VA's Talent Management System (TMS). Background investigation and adjudication is completed on contract personnel serving in this role. Contractors will be given access to commit code to the application and complete their contractual obligations. Contractors' credentials and certifications are reviewed quarterly by the Contract Officer Representative (COR).

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

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

All VA employees and contractors are required to go through the following VA TMS training course:
•Privacy & HIPAA training
•VA Privacy and Information Security Awareness and Rules of Behavior Training

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

If Yes, provide:

1. *The Security Plan Status, Approved*
2. *The Security Plan Status Date, 14-Nov-2019*
3. *The Authorization Status, Authorization to Operate (ATO)*
4. *The Authorization Date, 17-Jan-2020*
5. *The Authorization Termination Date, 16-Jan-2023*
6. *The Risk Review Completion Date, 31-Dec-2019*
7. *The FIPS 199 classification of the system (MODERATE).*

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.***

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.

Yes, ARMS is a VA Enterprise Cloud (VAEC),system.

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.

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met?

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

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

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

KARY CHARLEBOIS

Digitally signed by KARY CHARLEBOIS
Date: 2022.12.04 17:42:45 -05'00'

Privacy Officer, Kary Charlebois

Pamela R. Crockett-Williams 1555457

Digitally signed by Pamela R. Crockett-Williams 1555457
Date: 2022.12.06 16:39:33 -05'00'

Information Systems Security Officer, Pamela Crockett-Williams

Eric L. Hickam 164701

Digitally signed by Eric L. Hickam 164701
Date: 2022.12.05 09:58:59 -06'00'

Information System Owner, Eric Hickam

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).

44VA01 SORN https://www.govinfo.gov/content/pkg/FR-2013-11-06/pdf/2013-26522.pdf
The log on screen will also have the following message:
"You are accessing a U.S. Government information system, which includes:
(1)this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only. Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties. By using this information system, you understand and consent to the following:

You have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system. At any time, the government may for any lawful government purpose monitor, intercept, search and seize any communication or data transiting or stored on this information system. Any communications or data transiting or stored on this information system may be disclosed or used for any lawful government purpose."