Privacy Impact Assessment for the VA IT System called:

Salesforce - Veterans Account Management System Debt Management Center

Veterans Affairs Central Office

Enterprise Program Management Office

eMASS ID #1887

Date PIA submitted for review:

10/28/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Gina Siefert	Gina.Siefert@va.gov	224-558-1584
Information System Security Officer (ISSO)	James Boring	James.Boring@va.gov	215-842- 2000 Ext: 4613
Information System Owner	Michael Domanski	Michael.Domanski@va.gov	727-595-729

Abstract

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

The Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC) relates to the Veterans Account Management System (VAMS) which is used by the Debt Management Center (DMC). VAMS is the existing case management tool in use by the DMC to service Veteran debt needs. The DMC is expanding its Salesforce VAMS Application that is currently fielded to support changes due to the Veterans Benefits Administration (VBA) Enterprise Management of Payment Workflow and Reports (EMPWR) Modernization.

The VAMS DMC module has three main components: Salesforce, S-Docs and MuleSoft. The DMC backend updates VAMS each morning with a minimal debt record by calling Salesforce Application Programming Interface (APIs). Data is stored on the custom debt record and UUU (Unassociated, Unidentified, Unapplied) objects in Salesforce. Debt data from the DMC backend system is read-only in Salesforce. VAMS also supports Customer Service Representatives (CSR) with Case Management. Case management process includes the ability for CSR to create cases against existing Debts. All communications between VAMS and the DMC backend systems for data display and data updates are performed using real time web service API's hosted in the VA's Austin Information Technology Center (AITC) environment. VAMS DMC is hosted in the Salesforce Government Cloud.

There are three connections to the system: Centralized Accounts Receivable System (CARS), VA Master Person Index (MPI), and VA Profile. The backend of Salesforce DMC integrates with Digital Veteran's Platform (DVP) to access data from the VA's Master Person Index (MPI), which is the authoritative source for veteran identity information. Integration between MPI and Salesforce which includes both calls from VAMS and call from DVP Debt-to-Contact Integration batch job uses a set of APIs (sfdc-mpi-ent) deployed in support of the MPI Enterprise Integration project (Java library).

Overview

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

1 General Description

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

The Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC) relates to the Veterans Account Management System (VAMS) which is used by the Debt Management Center (DMC). VAMS is the existing case management tool in use by the DMC to service Veteran debt needs. The DMC is expanding its Salesforce VAMS Application that is currently fielded to support changes due to the

Veteran Benefits Administration (VBA) Enterprise Management of Payment Workflow and Reports (EMPWR) Modernization.

The expanded functionality of VAMS includes enhancements to address legislative changes under the Veterans Benefits Administration, enabling the DMC to better align with the VA's missions of delivering exceptional service to veterans. By modernizing and improving the DMC's debt management capabilities, the system helps maintain accountability while supporting veterans in managing their financial obligations. This case management tool is integral to ensuring veterans receive fair and efficient resolution.

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

Salesforce Government Cloud Plus - Enterprise (SFGCP-E) is a cloud platform. Data in the platform is VA Controlled / non-VA Owned and Operated.

2. Information Collection and Sharing

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

The Veteran Account Management System Debt Management Center (VAMS DMC) will store and/or pass through between 1,000,000 and 9,999,999 Veterans and their dependent related data.

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

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

Personally Identifiable Information (PII) maintained in the system is used for purposes of collecting debt receivables. The primary services of the VAMS DMC entail the receipt, processing, tracking and disposition of Veterans benefits and requests for assistance to aid in the determination of potential debt due to overpayment.

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

VAMS DMC system has three internal connections in which information is shared by leveraging: Debt Management Center's (DMC's) Centralized Accounts Receivable Systems (CARS), Master Person Index (MPI), and VA Profile.

Internal information sharing is conducted between Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC) and MuleSoft, Salesforce, S-Docs. There is two-way integration from Intermediate Database (IMDB) to Salesforce via MuleSoft. IMDB is the SQL server database that has a copy of CARS Data which is a mainframe system. It is different from the VA Enterprise Program Management Development (EPMD) which is used by Financial System Central Accounts Receivable System (CARS). Data will be stored on the custom debt and UUU (Unassociated, Unidentified, Unapplied) objects in Salesforce. S-Docs is a Salesforce AppExchange app that will store and generate letter templates. DMC Staff will use the Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC) minor application to build, generate, edit, save, and print letters to Veterans regarding Veteran debt obligations to VA. Debt records will be stored as read-only in Salesforce.

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

Yes

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

No, VAMS DMC is not operated in more than one site.

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

H. What is the citation of the legal authority?

88VA244 / 83 FR 40140, *Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO)* (8/13/2018)
https://www.govinfo.gov/content/pkg/FR-2018-08-13/pdf/2018-17228.pdf

VAMS DMC will replace CAROLS in the future. The SORN will be updated to add VAMS and update the data retention dates**.**

The legal authority to operate comes from 38 CFR §1.900 et seq. are the VA claims standards; Federal Claims Collection Standards, 31 CFR CH. IX and Parts 900, et al; PL94-466, The Veterans Rehabilitations and Education Amendments of 1980 as amended: The Debt Collection ACT of 1982 (PL97-365).

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Government records are maintained and managed under the authority set forth in 31 U.S.C. 3101 and 31 U.S.C. 3102. The purpose of the system is consistent with the financial management provisions of title 31, United States Code, chapter 37, the pay administration provisions of title 5, United States Code, chapter 55, and special provisions relating to VA benefits in title 38, United States Code, chapter 53.

I. What is the SORN?

88VA244 / 83 FR 40140, *Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO) (8/13/2018)*
https://www.govinfo.gov/content/pkg/FR-2018-08-13/pdf/2018-17228.pdf

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

Yes, SORN 88VA244 / 83 FR 40140 does require a modification.

4. System Changes

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

☐ Yes
☒ No
if yes, <<ADD ANSWER HERE>>

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

☐ Yes
☒ No
if yes, <<ADD ANSWER HERE>>

Section 1. Characterization of the Information

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

1.1 Information collected, used, disseminated, created, or maintained in the system.

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

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

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

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

- ☒ Name
- ☒ **Full** Social Security Number
- ☐ **Partial** Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☒ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a Different Individual)
- ☒ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account Numbers
- ☐ Certificate/License Numbers[1]
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☐ Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☒ Gender/Sex
- ☒ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☒ Date of Death
- ☐ Business Email Address
- ☐ Electronic Data Interchange Personal Identifier (EDIPI)
- ☒ Other Data Elements (List Below)

Other PII/PHI data elements: File Number, ADAM Key (Unique Identifier for Debt Record in VAMS DMC System), Receivable ID (Unique Identifier for Debt Record in VAMS DMC system), Recipient ID,

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

Participant ID, Beneficiary ID, Stub name (Truncated First/Last Name and Middle Initial), Work Phone Number, Cell Phone Number

1.2 List the sources of the information in the system

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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

The information collected does not come from an individual. The information is collected from Centralized Accounts Receivable Systems (CARS).

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.

The information is collected from Centralized Accounts Receivable Systems (CARS) because it is the source of Veteran or beneficiary debt information.

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

No, the system does not create information.

1.3 Methods of information collection

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

Information for VAMS DMC is collected via electronic transmission from internal VA systems, primarily the centralized accounts receivable system (CARS). VAMS DMC does not directly collect information from individuals nor does it generate or create data on its own. The data obtained through these integrations supports the systems functionality and managing and processing veterans' debt obligations.

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?

VAMS DMC does not collect information on a form.

1.4 Information checks for accuracy, and how often will it be checked.

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

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

Information accuracy is checked daily. VAMS DMC customer service representative's day to day job is to create a case against existing debts. The case may involve just a debt review or possibly updates to debt and/or payee information.

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?

VAMS DMC does not check accuracy by accessing a commercial aggregator of information.

1.5 Identify the specific legal authorities, arrangements, and agreements that defined the collection of information.

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

The legal authority to operate comes from 38 CFR §1.900 et seq. are the VA claims standards; Federal Claims Collection Standards, 31 CFR CH. IX and Parts 900, et al; PL94-466, The Veterans Rehabilitations and Education Amendments of 1980 as amended: The Debt Collection ACT of 1982 (PL97-365).

VAMS DMC is governed by Veterans Affairs System of Record Notice (VA SORN): 88VA244 / 83 FR 40140, *Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO)* https://www.govinfo.gov/content/pkg/FR-2018-08-13/pdf/2018-17228.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: *The collection ties with the purpose of the underlying mission of the organization and its enabling authority.*

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: The system collects Personally Identifiable Information (PII) from source systems and not from individuals. There is a risk that information contained within the systems could be inaccurate.

Mitigation: DMC has an integration with the source system. Any inaccurate information will be updated by the authoritative system of record. DMC will retrieve all updates from the Master Person Index (MPI). However, DMC updated data will not be processed at MPI. DMC also receive telephonic requests and written correspondence from the debtors verifying their PII prior to any manual action or update.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
Name	Used for validating identity	N/A
Full Social Security Number	Used as look-up and connection to a debtor through the entire Department of Veterans Affairs (not DMC specific)	N/A

Date of Birth	Used to assist in validating a caller identity	N/A
Personal Mailing Address	To send correspondence and assist in validating a caller identity	N/A
Personal Phone Number(s)	Stored in the event of a call back (to call a customer) and assist in validating a caller identity	N/A
Work Phone Number	Stored in the event of a call back (to call a customer) and assist in validating a caller identity	N/A
Cell Phone Number	Stored in the event of a call back (to call a customer) and assist in validating a caller identity	N/A
Personal Email Address	Assists in validating a caller identity and correspondence	N/A
Financial Information	Payment information	N/A
Gender/Sex	File Identification purposes	N/A
Integrated Control Number (ICN)	Used as individual identifier	N/A
Date of Death	Collecting for debt from individuals who are deceased	N/A
File Number	A unique identifier that is used to verify who the debtor is	N/A
ADAM Key (Unique Identifier for Debt Record in VAMS DMC System)	Used as an identifier per person per debt between Salesforce and DMC back-end (CARS/IMDB)	N/A
Receivable ID (Unique Identifier for Debt Record in VAMS DMC System)	Identifier per debt between Salesforce and DMC back-end (CARS/IMDB)	N/A
Recipient ID	Used as an identifier per person per debt between Salesforce and DMC back-end	N/A

Participant ID	Used as an identifier per person per debt between Salesforce and DMC back-end	N/A
Beneficiary ID	Used as an identifier per beneficiary per debt between Salesforce and DMC back-end	N/A
Stub Name (Truncated First/Last Name and Middle Initial)	Used for validating identity	N/A

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

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

VAMS DMC helps create collection notices and payment information related to the debt collection process. It regularly receives updates from other systems such as CARS, MPI, and VA profile to keep account balances current. VAMS DMC is not a long-term storage system; it is a tool for managing and processing data while all permanent records and analysis are handled by the original system where the data came from.

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.

This system performs different actions on UUU records. Examples of actions include: Apply (420), Refund (410), Return to Appropriation/MISC (410), Transfer to Station (410), and Insert/Admin Correction (411). Letters to Veterans concerning the progress of their potential debt reclamation are generated periodically as well as requests for additional information to substantiate the claim. These letters are generated electronically, printed on paper, and mailed to the Veterans.

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

2.3a What measures are in place to protect data in transit and at rest?
The DMC VAMS system is hosted in the vendor owned Amazon Web Services (AWS) Gov cloud which is Federal Risk and Authorization Management Program (FedRAMP) certified ensuring compliance with federal security standards for safeguarding stored data. Data in transit is protected through two-way SSL (secure socket layer) and transport layer security (TLS) protocols. Additionally, the Salesforce Shield product provides Federal Information Processing Standards (FIPS) 140 to certified encryption to secure data at rest. Data exchanges with systems such as CARS, VA profile, and MPI are encrypted ensuring secure electronic transmission.

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

Social Security Numbers (SSN) are encrypted and only available to certain users.

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

Use of secure passwords, access on a need-to-know basis, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized to safeguard PII/PHI data

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?

All information collected in this system is handled in accordance with policies and procedures related to information security. All persons granted access to VA systems are granted that access based on their position, duties, and a job related need-to-know.

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

Access to the VAMS DMC system is requested by the employee's supervisor and approved by the system owner through the Digital Transformation Center (DTC). All users will be required to authenticate to the system with a PIV card and will only have permissions to perform their assigned function. Based upon that function, each user will only have access to information on those participants which are assigned to them by their manager. The system will perform extensive logging to detail all actions taken by a user. Some of these actions are (but not limited to): Logon / Logoff, Create Data, Update Data, and Delete Data.

2.4c Does access require manager approval?

Yes

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

Yes, access to PII within VAMS DMC is monitored, tracked, and recorded. The system includes electronic safeguards that log users' activity, monitors access attempts and it tracks actions performed on sensitive data to ensure compliance with security protocols.

These controls are design to further protect sensitive information collected by VA from inadvertent disclosure and/or malicious disclosure.

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

DMC employs an Information System Security Officer whose duty is to audit user accounts, system roles, and security violations of DMC personnel, and to ensure appropriate security levels are assigned.

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*

The system will retain Veteran payment information and PII to include: Name, Full Social Security Number, Date of Birth, Personal Mailing Address, Personal Phone Number(s), Personal Email Address, Financial Information, Gender/Sex, Integrated Control Number (ICN), Date of Death, File Number, ADAM Key (Unique Identifier for Debt Record in VAMS DMC System), Receivable ID (Unique Identifier for Debt Record in VAMS DMC system), Recipient ID, Participant ID, Beneficiary ID, Stub name (Truncated First/Last Name and Middle Initial), Work Phone Number, and Cell Phone Number

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

Financial transaction records related to procuring goods and services, paying bills, collecting debts, and accounting are retained temporarily. These records are destroyed six years after final payment or cancellations unless longer retention is required for business purposes. However, Salesforce retains information indefinitely within the system and does not delete it unless a specific request for deletion is made and ensuring compliance with retention policies and business's needs.

3.3 The retention schedule approved by the VA records office and the National Archives and Records Administration (NARA).

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

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

Yes

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

General Records Schedule 1.1: Financial Management and Reporting Records
Item 010, Disposition Authority DAA-GRS-2013-000-0001
https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

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.

Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC) tool adheres to the VA RC Schedule 10-1. All electronic storage media used to store, process, or access records will be disposed of in adherence with the VA Directive 6500. (https://www.va.gov/vapubs/search_action.cfm?dType=1).

Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction. https://www.va.gov/vapubs/search_action.cfm?dType=1

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.

The use of PII during research, testing, and training is reduced, when possible, to minimize risk. PII is not used in research. PII is minimally used in testing and training when de-identifier data is not able to be used due to system constraints. In instances of testing and training that contain PII, adherence to VA Handbook 6500 is followed.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

Principle of Minimization: The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.

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

Follow the format below:

Privacy Risk: PII may be held for long after the original record was required to be disposed of. The extension of retention periods increases the risk that SPI may be breached or otherwise put at risk.

Mitigation: The privacy risk is mitigated by retaining the information in accordance with the approved NARA retention schedules. The security controls in place for Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC) follow VA Handbook 6500 and 6301 as well as NIST 800-53 moderate impact defined set of controls.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

PII Mapping of Components

4.1a Veterans Account Management System Debt Management Center (VAMD DMC) consists of 1 key components (servers/databases/instances/applications/software/application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Veterans Account Management System Debt Management Center (VAMD DMC) and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
VAMS Salesforce APP	Yes	Yes	• Name • Social Security Number • Date of Birth	Proper identification and processing of Veteran files.	Use of secure passwords, access on a need-to-know basis, Personal Identification

			• Personal Mailing Address • Financial Information • Integrated Control Number (ICN) • Date of Death • File Number • ADAM Key • Receivable ID • Recipient ID • Participant ID • Beneficiary ID Stub Name		Numbers (PIN), encryption, and access authorization are all measures that are utilized to safeguard PII/PHI data.

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

NOTE: Question 3.9b (second table) on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
Debt Management Center's (DMC's) Centralized Accounts Receivable Systems (CARS)	To review Veteran information and to send correspondence.	• Name • Social Security Number • Date of Birth • Personal Mailing Address • Date of Death • File Number • ADAM Key • Receivable ID • Recipient ID • Stub Name • Participant ID	Two-way SSL Integration
VA Identity and Service Services Master Person Index (MPI)	To review Veteran information and to send correspondence.	• Name • Social Security Number • Date of Birth • Personal Phone Number(s) • Gender	Electronically Pulled from VHA. Web Service With Mutual TLS Authentication
VA Profile	To review Veteran information and to send correspondence.	• Personal Mailing Address • Personal Phone Number(s) • Work Phone Number • Cell Phone Number • Personal Email Address	Electronically Pulled from VA Profile. Web Service With Mutual TLS Authentication

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: Privacy information may be released to unauthorized individuals.

Mitigation: All personnel with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually. The Debt Management Center adheres to all information security requirements instituted by the VA Office of Information Technology (OIT). Information is shared in accordance with VA Handbook 6500. Windows and Unix access controls are provided by VA's Infrastructure Operations (IO) along with the following security controls: Audit and Accountability, Awareness Training, Security Assessment and Authorization, Incident Response, Personnel Security, and Identification and Authentication.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

List IT System or External Program Office information is shared/received with	***List the purpose of information being shared / received / transmitted***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)***	***List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
N/A	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

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

Follow the format below:

Privacy Risk: There is no external sharing.

Mitigation: There is no external sharing.

Section 6. Notice

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

6.1 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms,

notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.

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

6.1a Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.

The PII is collected from other systems, Centralized Accounts Receivable System (CARS) that have collected the PII/PHI. Information was collected for use in those upstream systems and notice was provided at that time.

The SORN also serves as a Privacy Notice - 88VA244 / 83 FR 40140 Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO)
https://www.govinfo.gov/content/pkg/FR-2018-08-13/pdf/2018-17228.pdf

This Privacy Impact Assessment (PIA) also serves as notice of the Debt Management Center General Support System. As required by the eGovernment Act of 2002, Pub.L.107-347 208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register." The Department of Veterans Affairs provides notice through the publication of the VA System of Record Notice (VA SORN). VAMS DMC receive data from CARS. All PIAs are available to the public at
https://department.va.gov/privacy/privacy-impact-assessments/

6.1b If notice was not provided, explain why.

Notice is provided in the form of publicly available SORN and PIA (see answer to 6.1a). Notice is provided through SORN, 88VA244 / 83 FR 40140 Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CARS/CAROLS, Combined system referred to as CAO). VAMS DMC will replace CAROLS in the future. The SORN will be updated to add VAMS and update the data retention dates**.**
2018-17228.pdf (govinfo.gov)

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

The notice provided at the time of collection as outlined in SORN, 88VA244 / 83 FR 40140 for the Centralized Accounts Receivable System (CAROLS), meets the purpose of use for the system by describing the collection, use, and retention of information required to manage accounts receivable and related debt collection activities. As VAMS DMC replaces CAROLS, the updated SORN will reflect the expanded billing capabilities, updated retention schedules, and system functionalities to ensure alignment with the stated purpose of managing veterans' debt obligations effectively and securely.

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.

Individuals do not directly provide information to VAMS DMC. The system collects data from existing VA systems (e.g.,CARS, MPI, and VA profile) via interconnections. However, the information in those systems is typically required to process the services provided by the VA. If an individual declines to provide their information during their initial interaction with those systems, it may result in limited or no access to VA services as their data is needed to manage benefits, records, and other services.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses, or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

Once information is provided to the VA, the records are used as necessary to ensure the administration of debt collection to Veterans, Service members, reservists, and their spouses, surviving spouses and dependents. As such, the Debt Management Center does not provide individuals with the direct opportunity to consent to particular uses of information on the General Support System (GSS). However, if an individual wishes to remove consent for a particular use of their information, they should contact the Debt Management Center at 1-(800) 827-0648.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Follow the format below:

Privacy Risk: Privacy information may be collected prior to providing written notice.

Mitigation: The VA mitigations this risk by providing Veterans and other beneficiaries with multiples forms of notice of information collection, retention, and processing. The two main forms of notice are discussed in detail in question 6.1 and include a System of Record Notice and the publishing of this Privacy Impact Assessment.

Section 7. Access, Redress, and Correction

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

7.1 The procedures that allow individuals to gain access to their information.

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

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

88VA244 / 83 FR 40140, *Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO)* https://www.govinfo.gov/content/pkg/FR-2018-08-13/pdf/2018-17228.pdf

Per SORN 58VA21/22/28 / 86 FR 61870 as reference from 88VA244, individuals seeking information regarding access to and contesting of VA records should mail their Privacy Act or FOIA requests to: Department of Veterans Affairs, Claims Intake Center, P.O. Box 4444, Janesville, WI 53547–4444, DID: 608–373–6690.

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)?

VAMS DMC 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?

VAMS DMC is a Privacy Act system.

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

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

88VA244 / 83 FR 40140, *Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO)*
https://www.govinfo.gov/content/pkg/FR-2018-08-13/pdf/2018-17228.pdf

Per SORN 58VA21/22/28 / 86 FR 61870 as reference from 88VA244, individuals seeking information regarding access to and contesting of VA records should mail their Privacy Act or FOIA requests to: Department of Veterans Affairs, Claims Intake Center, P.O. Box 4444, Janesville, WI 53547–4444, DID: 608–373–6690.

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.

Veterans and other beneficiaries are notified of the procedures for correcting their records at the VA through VA SORN *Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA.* The SORN directs individuals seeking information regarding access to and contesting of VA records to write or call the Debt Management Center at 1-800-827-0648. The mailing address is Department of Veterans Affairs, Claims Intake Center, P.O. Box 4444, Janesville, WI 53547–4444, DID: 608–373–6690.

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.

Individual wishing to obtain more information about access, redress and record correction of Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records should contact the Department of Veteran's Affairs Veterans Benefits Administration at 1-800-827-1000. Veterans Services Representatives are available from 7:00 AM to 7:00 PM (Eastern Time), Monday thru Friday, except for federal holidays. For more information – see https://benefits.va.gov/benefits/

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that individuals may attempt to access or redress records about them held by the VA office and encounter challenges due to incorrect or incomplete records. This could potentially lead to concerns about data accuracy or privacy compliance.

Mitigation: By publishing this PIA, and the applicable SORN, the VA makes the public aware of the unique status of applications and evidence files, such as those stored on the Veterans Benefits Management System (VBMS) and Virtual VA platforms. NOTE: The data from Virtual VA was included in VBMS and Virtual VA is now decommissioned. Furthermore, this document and the SORN provide.

Section 8. Technical Access and Security

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

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

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

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

Access to the system is managed through a formal process. Managers request access for users based on their roles and responsibilities. These requests are reviewed to ensure they are aligning

with security needs and administrators grant access to only the necessary permissions. Access is reviewed periodically to ensure it remains appropriate.

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?

There are no users from other non-VA agencies with access to VAMS DMC system.

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.

VAMS DMC users have access privileges identified by their supervisors as needed to perform their assigned duties. The Requesting Official is responsible for ensuring that the user's access is restricted to only those applications and functions that are required for the user to perform their assigned duties and that separation of duties has been applied as appropriate.

8.2. Contractor signed Non-Disclosure Agreement (NDA), Business Associate Agreement (BAA) etc. in place.

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.

8.2a Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

VA contract employee access is verified through the Contracting Officer's Representative (COR) and other VA supervisory/administrative personnel before access is granted to any VA system. Contractor access is reviewed annually at a minimum. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of Behavior (ROB) training via the VA Talent Management System (TMS). All contractors are vetted using the VA background investigation process and must obtain the appropriate level background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access. Generally, contracts are reviewed at the start of the initiation phase of acquisitions and again during procurement of option years by the Contracting Officer, Information Security Officer, Privacy Officer, COR, Procurement Requestor/Program Manager, and any other stakeholders required for approval of the acquisition. Contracts generally have an average duration of 1-3 years and may have option years stipulated in the original contract.

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

Contractors may have access to the system in limited capacity. However, they do not have direct access to PII. Access is strictly managed and subject to VA compliance and security protocols.

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

Contractors may have limited access to the system during the enhancement process to support configuration, updates, and testing. All contractor work is performed in compliance with VA security and privacy requirements including the signing of confidentiality agreements such as Rules of Behavior (ROB) to ensure proper handling of sensitive data. Contractors do not have unrestricted access to production environment and work primarily with test or dummy data to ensure privacy and data security.

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 individuals granted access to this system are required to have extensive training prior to receiving access and are required to recertify annually that he/she understands VA's commitment to continuous readiness in information security. This annual training, which is coalesced under the title of "Continuous Readiness in Information Security Program" (CRISP), is a VA initiative designed to increase security for information that is contained in this system as well as all other VA systems. A cornerstone of CRISP is that all VA employees have a direct personal responsibility to safeguard the privacy of Veterans and to ensure sensitive information remains protected.

This responsibility extends to VA contractors, volunteers at VA facilities, trainees and others who deal with Veterans' information at VA. CRISP builds upon VA's long-standing security policies by ensuring consistent centralized training on IT security, records security, and privacy awareness. Most of this web-based training is self-paced, interactive, and requires employees to answer questions correctly before they can proceed. The program also tracks the progress of employees and identifies trends where additional training may be necessary. Employees who fail to complete this annual training or adhere to the "Rules of Behavior" outlined in CRISP training will have their system access/IT privileges, and record access removed.

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

8.4a If completed, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 06/05/2023
3. *The Authorization Status:* Approved

4. *The Authorization Date:* 06/05/2023
5. *The Authorization Termination Date:* 6/13/2026
6. *The Risk Review Completion Date:* 6/13/2023
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 not completed or In Process, provide your ***Initial Operating Capability (IOC) date***

Section 9 – Technology Usage

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

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

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties. ***(Refer to question 1.8 of the PTA)***

Yes, VA has full ownership of the PII/PHI that will be shared through VAMS DMC. Contract agreement "Salesforce Subscription Licenses, Maintenance and Support", Contract Number: NNG15SD27B, Order Number: 36C10B23F0172.

Salesforce Government Cloud Plus (SFGCP) is hosted in AWS GovCloud. The SFGCP is the PaaS platform for all the minor application for SaaS to operate on.

9.2 Does the contract with the Hosting Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.1 of the PTA)* *This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

A Memorandum of Understanding and Interconnection Security Agreement (MOU/ISA) between VA and Salesforce identifies the data flow and responsibilities of both parties. Data is owned by the VA and is stored at Salesforce based on VA guidelines.

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.

No, VAMS DMC does not collect any ancillary data.

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.

Yes, this principal is included in the VA contracts with service providers. These contracts make sure the VA stays in control of the data stored in the Veterans Electronic Records Archive (VERA) system and that privacy and security requirements are followed.

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).

No, VAMS DMC does not utilize Robotics Process Automation (RPA).

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.

GINA SIEFERT Digitally signed by GINA SIEFERT
Date: 2025.02.10 11:13:39 -06'00'

Privacy Officer, Gina Siefert

JAMES BORING Digitally signed by JAMES BORING
Date: 2025.02.18 12:57:19 -05'00'

Information System Security Officer, James Boring

MICHAEL DOMANSKI Digitally signed by MICHAEL DOMANSKI
Date: 2025.02.18 10:54:15 -05'00'

Information System Owner, Michael Domanski

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).

88VA244 / 83 FR 40140, *Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO)*
https://www.govinfo.gov/content/pkg/FR-2018-08-13/pdf/2018-17228.pdf

PIA webpage:
https://department.va.gov/privacy/privacy-impact-assessments/

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

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

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

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

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

Notice of Privacy Practice (NOPP):
VHA Directive 1605.04
IB 10-163p (va.gov)