Privacy Impact Assessment for the VA IT System called:

Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC)

Enterprise Program Management Office (EPMO)

Veterans Affairs Central Office (VACO)

Date PIA submitted for review:

June 16, 2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Tonya Facemire	tonya.facemire@va.gov	202-632-8423
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	727-595-7291

Abstract

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

The Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC) minor application has three main components: MuleSoft, Salesforce, and S-Docs. Data will be stored on the custom debt object 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. Examples of data used will include Veteran name, address, contact information, type of debt, and amount of debt. This is hosted in the Salesforce Government Cloud.

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?*

The IT system name: The Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC)
The Name of the program office that owns the IT system: Enterprise Product Management Office (EPMO)

The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission:

Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC) is designed to assist in the collection of Veterans Affairs related over-payments and to provide the DMC with reports and statistical data on the volume and characteristics of over-payments.

Indicate the ownership or control of the IT system or project: VA Debt Management Center (DMC)

The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual:

Salesforce - Veterans 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 dependents related files.

A general description of the information in the IT system and the purpose for collecting this information:

Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC) supports Custom Service Representative's (CSR) with Case Management. Case management process includes the ability for CSR to create cases against existing Debts. The case may involve just a debt review or possibly updates to debt and/or payee information. The custom debt object has been extended with 12 extra fields to support Case Management operations. In addition, several components have been developed to display remote debt information currently stored in CAROLS backend system and documents stored in FileNet. The project also extended Mule integrations to deliver S-Doc letter to FileNet. Finally, custom components will be developed to allow CSR to generate updates to debt and/or personal information; perform 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). Updates will be delivered to CAROLS transaction table for processing. All communications between Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC) and CAROLS for data display and data updates are performed through using real time web service APIs developed on Mule runtime engine or platform (middleware solution), which is hosted in VA Austin Information Technology Center (AITC) environment. Cloud technology is used and Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC) is hosted in the Salesforce Government Cloud (FedRAMP). Salesforce Government Cloud Assessing (FedRAMP) authorization was granted a VA Authority to Operate (ATO) valid through 06/04/2020. Connection to the Salesforce was documented and approved under VA Cyber Security Operations Center (CSOC) Trusted Internet Connection (TIC) Business Partner Extranet (BPE) Connection ID B0320. 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. Salesforce has the responsibility of notifying VA of actual or reasonably suspected unauthorized disclosure of VA Data by Salesforce or those acting on its behalf.

Salesforce - Veterans Account Management System Debt Management Center (VAMS 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 call from Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC) GUI 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). Following functionalities are supported by the MPI Enterprise APIs:

- Attended Search Person - MPI Performs a probabilistic search and calculates a "match score" based on the set of traits submitted (query parameters) that include Last Name, First Name, Date of Birth, SSN, Gender, and Phone Number. A potential match must exceed a score threshold set in MPI to be returned.
- Unattended Search Person - Same as the Attended Search Person above but with a parameter set indicating "unattended." In this case MPI returns only a single match.
- Retrieve Person - Returns the same information as Attended/Unattended Search Person, but a well-known unique identifier is provided instead of identity. The unique identifiers currently supported by DVP MPIe are Integration Control Number (ICN), File Number, and Salesforce Id.
- Correlate Person - This API correlates or "maps" a Salesforce Contact Id to an MPI ICN.

VA Profile is the source system for the Veteran's and dependents address information. This information will be used by DMC for correspondence. DMC GUI call will send Contact ID that was correlated with the MPI and the API would in turn use that to get the appropriate VA Profile ID from MPI. Subsequently, the API will use the VA Profile ID to retrieve the VA profile information for the person from VA profile system. It is important that the Salesforce contact MUST have been previously correlated to the ICN. If a contact was not correlated with ICN that means the contact isn't verified in the VAMS DMC system.

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

Internal information sharing is conducted between Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC) and MuleSoft, Salesforce, S-Docs, and Intermediate Database (IMDB)/Centralized Accounts Receivables On-Line System (CAROLS). External information sharing is conducted between Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC) and Salesforce Government Cloud (FedRAMP). Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC) is governed by Veterans Affairs System of Record Notice (VA SORN) Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CARS/CAROLS, Combined system referred to as CAO) Records-VA

There is two-way integration from Intermediate Database (IMDB)/ Centralized Accounts Receivables On-Line System (CAROLS) to Salesforce via MuleSoft. IMDB is the SQL server database that has a copy of CAROLS 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. Examples of data used will include Veteran name, address, contact information, type of debt, and amount of debt. Unassociated, Unidentified, Unapplied data from IMDB is stored in UUU records in salesforce. Examples of data used include
UUU Amount, file number, deposit number, Adam key, payee code, deduction code, and payment received date.

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:
Veterans Account Management System Debt Management Center (VAMS DMC) not operated in more than one site

A citation of the legal authority to operate the IT system:
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).

Whether the completion of this PIA will result in circumstances that require changes to business processes:
Completion of this PIA not required changes to business process

Whether the completion of this PIA could potentially result in technology changes:
Completion of this PIA will not require changes 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?: SORN 88VA244 updated 08/13/2018. https://www.govinfo.gov/content/pkg/FR-2018-08-13/pdf/2018-17228.pdf. Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC) will replace CAROLS at an unknown date in the future but will still receive data from CARS. The SORN will be updated to add Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC) and update the data retention dates.

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)

In Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC), on the Debt records following data elements (PII) is stored so that Letters can be generated accurately:

- Address Line 1
- Address Line 2
- Address Line 3
- Address Line 4
- ADAM Key (Unique identifier for a Debt record in Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC) system.)
- Date Of Birth
- File Number
- First Name
- Last Name
- Middle Name
- City
- Zip

Additionally, to support Case Management operations SSN (PII) information saved on debt records is use On UUU record following data element is stored to perform different action on which include Apply (420), Refund (410), Return to Appropriation/MISC (410), Transfer to Station (410), and Insert/Admin Correction (411)

- UUU Amount
- file number
- deposit number
- Adam key
- payee code
- deduction code
- payment received date.

MPI Enterprise APIs
Attended/Unattended Search Person APIs use following query parameters:

- Last Name
- First Name
- Date of Birth
- SSN
- Gender
- Phone Number

Retrieve and Correlate person APIs use following query parameters:

- ICN
- File Number

VA Profile
Following data is obtained by querying backend web service API's that extract the data from VA Profile:

- Address(es) - Correspondence and Residence Choice
- Phone Numbers - Work, Home, Mobile
- Email

PII Mapping of Components

Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC) consists of 1 key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC) and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

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

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
DMC IMDB	**Yes**	**Yes**	Name, DOB, Social Security Number, Address, Phone Num, File Number, UUUAmount,	PII is required for proper identification and processing of Veteran fil	Encryption

			depositNumber, ADAM Key (Unique identifier for a Debt record in VAMS DMC system.)		

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.

Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC) minor application has one main component: DMC IMDB. Sources of data include a two-way integration from Intermediate Database (IMDB)/Centralized Accounts Receivables On-Line System (CAROLS) to Salesforce via MuleSoft.

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 technologies 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.

Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC) does not originate the collection of data. Sources of data are obtained through one-way integration from the

following internal VA systems: Intermediate Database (IMDB)/Centralized Accounts Receivables On-Line System (CAROLS) to Salesforce via MuleSoft and Centralized Account Receivable System (CARS).

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.

Personally Identifiable Information maintained in the system is used for purposes of collecting debt receivables. The primary services of the Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC) entails the receipt, processing, tracking and disposition of Veterans benefits and requests for assistance to aid in the determination of potential debt due to overpayment. VAMS DMC custom 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. Information accuracy is checked daily.

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

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

The 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) Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CARS/CAROLS, Combined system referred to as CAO) Records-VA, SORN 88VA244 updated 08/13/2018. https://www.govinfo.gov/content/pkg/FR-2018-08-13/pdf/2018-17228.pdf. VAMS DMC will replace CAROLS at an unknown date in the future but will still receive data from CARS. The SORN will be updated to add VAMS and update the data retention dates.

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: The system collects Personally Identifiable Information (PII). Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional or financial harm may result for the individuals affected.

Mitigation: The system employs a variety of security measures designed to ensure that the information is not inappropriately disclosed or released. Electric safeguards and security controls are in place as well as access control, awareness and training, audit and accountability, certification, accreditation, etc. The system operates under guidance provided in the National Institute of Standards and Technology (NIST) Special Publication 800-37 and specific VA directives.

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 record, or information contained in the record, may include:

- Name: Used as individual identifier
- DOB: Used to identify individual age and to confirm individual identity
- Social Security Number: Used as individual identifier
- Address: Used to send mails to the individual for payment information
- Phone Number: Used to contact individual
- File Number: Used as individual identifier
- UUUAmount: Unassociated, Unidentified and Unapplied amount
- depositNumber: Payment information
- ADAM Key: Unique identifier for a Debt record for individual in VAMS DMC system

Salesforce - Veterans Account Management System Debt Management Center (VAMS 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 call from Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC) GUI 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). Following functionalities are supported by the MPI Enterprise APIs:

- Attended Search Person - MPI Performs a probabilistic search and calculates a "match score" based on the set of traits submitted (query parameters) that include Last Name, First Name, Date of Birth, SSN, Gender, and Phone Number. A potential match must exceed a score threshold set in MPI to be returned.
- Unattended Search Person - Same as the Attended Search Person above but with a parameter set indicating "unattended." In this case MPI returns only a single match.
- Retrieve Person - Returns the same information as Attended/Unattended Search Person, but a well-known unique identifier is provided instead of identity. The unique identifiers currently supported by DVP MPIe are Integration Control Number (ICN), File Number, and Salesforce Id.
- Correlate Person - This API correlates or "maps" a Salesforce Contact Id to an MPI ICN.

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

Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC) facilitates the generation collection notices and stores payment information as well as other data pertinent to the collection process. Data is received from IMDB/CARS/CAROLS/VA Profile on a reoccurring basis for the purpose of updating balances. Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC) acts as an integration platform to build and generate Veteran debt obligations to VA. Data created is not a permanent repository and is updated in the source system. Analysis will be conducted on source system.

Perform 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). Updates will be delivered to CAROLS transaction table for processing.

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 is the information in the system secured?

2.3a What measures are in place to protect data in transit and at rest?
Used BPE, Connection ID B0320 for secure transmission of the data.
Also, with two – way SSL transmission method

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?
SSNs 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 for need to know basis, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized to safeguarded PII/PHI data

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

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

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

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

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

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

Add answer here:

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. 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 Veteran, 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.

As system access is required as a condition of employment for DMC employees, those who lose access without taking action to complete training are subject to disciplinary action and/or risk dismissal. The system also includes electronic safeguards which further restrict access to certain information/data based on the security level of the information/record. Employees attempting to access that information must

have a security level which is equal or greater to the information being accessed.

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

Veteran payment information and PII to include Name, Address, Social Security Number, Date of Birth, Gender, Phone Number, Email, ICN, File Number, UUU Amount, Payment received date and ADAM Key is retained.

3.2 How long is information retained?

In some cases, the 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.

Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC) will retain data indefinitely. Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC) will replace CAROLS at an unknown date in the future but will still receive data from CARS. The SORN will be updated to add VAMS and update the data retention dates. All other automated storage media are retained and disposed of in accordance with VA or National Archives and Records Administration (NARA) as identified in SORN 88VA244 and will be updated to include Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC).

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.

Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC) will retain data indefinitely. Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC) will replace CAROLS at an unknown date in the future but will still receive data from CARS. The SORN will be updated to add VAMS and update the data retention dates. All other automated storage media are retained and disposed of in accordance with VA or National Archives and Records Administration (NARA) as identified in SORN 88VA244 and will be updated to include Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC). Please see the General Record Schedule located here: https://www.archives.gov/files/records-mgmt/grs/grs04-2.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

Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC) will replace CAROLS at an unknown future date, but will still receive data from CARS. The SORN will be updated to add VAMS and update the data retention dates. All other automated storage media are retained and disposed of in accordance with VA or National Archives and Records Administration (NARA) as identified in SORN 88VA244 and will be updated to include Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC).

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

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. 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.

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: PII may be held for long after the original record was required to be disposed. 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.

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***
EMPO - EPMD: Financial Services Center (FSC)	Debt Management Center's (DMC's) Centralized Accounts Receivable Systems (CARS)	Personally Identifiable Information (PII) and Data transmitted: debt owed by eligible Veterans and/or their dependents. o Address Line 1 o Address Line 2 o Address Line 3 o Address Line 4 o City o Zip Code o ADAM Key (Unique	Two-way SSL integration

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*
		identifier for a Debt record in VAMS DMC system.) o DOB o File Number o First Name o Middle Name o Last Name	
EPMO - EPMD: Financial Services Center (FSC)	Centralized Accounts Receivables On-Line System (CAROLS)	Personally Identifiable Information (PII) and Data transmitted: debt owed by eligible Veterans and/or their dependents. o Address Line 1 o Address Line 2 o Address Line 3 o Address Line 4 o City o Zip Code o ADAM Key (Unique identifier for a Debt record in VAMS DMC system.) o DOB o File Number o First Name o Middle Name Last Name	Two-way SSL integration
Office of Veterans Health Administration (VHA)	VA Identity and Service Services Master Person Index (MPI)	Personally Identifiable Information (PII), Sensitive Personal Information (SPI) and Individually Identifiable Information (III). ● Attended/Unattended Search Person APIs use following query parameters: Last Name, First Name, Date of Birth, SSN, Gender, and Phone Number ● Retrieve and Correlate person APIs use	Electronically pulled from VHA. System of record number (SORN#): 121VA10P2. MPI records are returned for specifically queried individuals via MPI's search services

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*
		following query parameters: ICN, File Number	
Office of Information Technology (OIT)	VA Profile	Personally Identifiable Information (PII) and Data transmitted: Person Contact Information – Consisting Of: ● Address(es) - Correspondence and Residence Choice ● Phone Numbers - Work, Home, Mobile Email	Electronically pulled from VA Profile. Web Service with Mutual TLS authentication.
EPMO - EPMD: Financial Services Center (FSC)	Centralized Accounts Receivables On-Line System (CAROLS)	Personally Identifiable Information (PII) and Data transmitted: Unassociated, Unidentified, Unapplied information consisting of: ● UUU Amount ● file number ● deposit number ● Adam key ● payee code ● deduction code payment received date	Two-way SSL integration

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: 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 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***	***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***	***List the method of transmission and the measures in place to secure data***

	office or IT system		***sharing (can be more than one)***	
Salesforce	The VA has embraced a "Cloud First" policy and Information Technology initiatives as established by the Chief Information Officer (CIO). Salesforce FedRAMP Government Cloud is used by U.S. Federal government Customers and is a chosen cloud provider by the VA.	Name, Address, Date of Birth, Social Security Number	MOU/ISA	BPE, Connection ID B0320

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

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

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

Follow the format below:

Privacy Risk: There is a risk that information may be shared with unauthorized VA Program or individual.

Mitigation: The safeguards implemented to ensure data is not sent to the wrong VA organization are employee security privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized.

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.

The Department of Veterans Affairs also provides notice by publishing the VA System of Record Notice (VA SORN) Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CARS/CAROLS, Combined system referred to as CAO) Records-VA, SORN 88VA244 (August 13, 2018), at the Federal Register and online. An online copy of the SORN can be found at https://www.govinfo.gov/content/pkg/FR-2018-08-13/pdf/2018-17228.pdf VAMS DMC will replace CAROLS at an unknown date in the future but will still receive data from CARS. The SORN will be updated to add Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC) and to update the data retention dates.

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."

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

Waivers, Compromises, Payment Plans and other information related to collection of a debt will not be processed without all of the requested information being provided. No allowance of debt relief may be granted unless this form is completed fully as required by law (38 U.S.C. 5101). The requested information is considered relevant and necessary to determine maximum benefits under the law. Information submitted is subject to verification through computer matching.

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 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.

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

Mitigation: The VA mitigates this risk by providing Veterans and other beneficiaries with multiple 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 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.

The following procedure is from the VA Handbook 6300.4:

(1) An individual may request amendment of a record pertaining to him or her contained in a specific VA system of records by mailing or delivering the request to the office concerned. The request must be in writing and conform the requirements in paragraph 3b(3) of this handbook. It must state the nature of the information in the record the individual believes to be inaccurate, irrelevant, untimely or incomplete; why the record should be changed; and the amendment desired. The requester should be advised of the title and address of the VA official who can assist in preparing the request to amend the record if assistance is desired.

(2) Not later than 10 days, excluding Saturdays, Sundays and legal public holidays, after the date of receipt of a request to amend a record, the VA official concerned will acknowledge in writing such receipt. If a determination has not been made, the acknowledgement will inform the individual when he or she may expect to be advised of action taken on the request. VA will complete a review of the request to amend or correct a record a soon as reasonably possible, normally within 30 days from receipt of the request (excluding Saturdays, Sundays and legal public holidays).

(3) Where VA agrees with the individual's request to amend his or her record(s), the requirements of 5 U.S.C. 552a(d) will be followed. The record(s) will be corrected promptly and the individual will be advised promptly of the correction. Amendment consists of adding information to the record, altering information in the record or deleting information in the record. Under the Privacy Act, if information is altered or deleted, the previous version must be obliterated and illegible after the amendment. The amendment should be annotated "Amended, Privacy Act, (date), (signature and title of amending official)."

(4) If the record has previously been disclosed to any person or agency, and an accounting of the disclosure was made, prior recipients of the record will be informed of the correction. FL 70-19, Notification to Other Person or Agency of Amendment to a Record, may be used.

(5) If it is determined not to grant all or any portion of the request to amend a record, the official will promptly notify the individual in writing. The individual will be advised of his or her right to file a concise statement of reasons for disagreeing with the refusal to amend. The notice will specify the reason(s) for denying the request, identify the VA regulations or statutes upon which the denial is based, and advise that the denial may be appealed in writing to the General Counsel (024), Department of Veterans Affairs, 810 Vermont Avenue, NW, Washington, DC 20420. FL 70-20, Notification of Initial Refusal to Amend a Record Under the Privacy Act, may be used for this purpose.

(6) The determination on an appeal will be made not later than 30 days, excluding Saturdays, Sundays, and legal public holidays, from the date the individual's letter of appeal is received unless the Secretary or Deputy Secretary, for good cause shown, extends such 30-day period. If the 30-day period is extended, the individual will be notified promptly of the reasons for the extension and the date on which a final determination may be expected. The final determination in such appeals will be made by the General Counsel or Deputy General Counsel.

(7) If the General Counsel or Deputy General Counsel finds that the adverse determination should be reversed, he or she will notify the VA office or station of the remedial action to be taken. The VA office or station will promptly carry out the action. The General Counsel or Deputy General Counsel will promptly notify the individual in writing of the corrective action. The field station or Central Office organization that provided the initial decision will inform previous recipients of the record that a correction has been made.

(8) If the General Counsel or Deputy General Counsel determines that the adverse determination will not be reversed, the individual will be notified promptly in writing of that determination, the reasons therefor, and of his or her right to seek judicial review of the decision pursuant to section 3of the Privacy Act (5 U.S.C. 552a9g)).

(9) If the adverse determination is sustained by the General Counsel or Deputy General Counsel, the individual will also be advised promptly of his or her right to file a concise statement of reasons for

disagreeing with the refusal to amend. The statement may contain information that the individual believes should be substituted.

(10) When an individual files a statement disagreeing with VA's decision not to amend a record, the record will be clearly annotated so that the fact that the record is disputed is apparent to anyone who may subsequently access, use, or disclose it. When the disputed record is disclosed to persons or other agencies, the fact of the dispute will be clearly noted. Copies of the statement of disagreement will be provided, and, when appropriate, copies of a concise statement of the VA's reasons for not making the amendment(s) requested will also be provided.

(11) A decision by either the General Counsel or Deputy General Counsel pursuant to paragraph 3f(7) of this handbook is final. It is subject to judicial review in the district court of the United States in which the complainant resides, or has his or her principal place of business, or in which the VA records are located, or in the District of Columbia.

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.

An individual has the right to request an amendment to any information or records retrieved by the individual's name or other individually identifiable information contained in a VA system of records, which includes designated record sets, as provided in 38 CFR 1.579 and 45 CFR 164.526. The right to seek an amendment of this information or records is a personal right of the individual to whom the record pertains.

The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief.

(1) The written request needs to be mailed or delivered to the VA health care facility that maintains the record.
(2) The individual must be asked to clarify a request that lacks specificity in describing the information for which an amendment is requested in order that a responsive decision may be reached.

A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and be filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579. That is, VA must maintain in its records only such information about an individual that is accurate, complete, timely, relevant, and necessary to accomplish a purpose of VA, as required by law, regulation, executive order of the President, or a government-wide or VA policy implementing such a purpose.

These criteria must be applied whether the request is to modify a record, to add material to a record, or to delete information from a record.

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

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Veterans and other beneficiaries are notified of the procedures for correcting their records at the VA through VA SORN Compensation, Pension, Education and Employment Records-VA, SORN 58VA21/22/28(July 19, 2012), which states: Records Access Procedures, Individuals seeking information regarding access to and contesting of VA records may write or call the Debt Management Center at 1-800-827-0648. The mailing address is Department of Veterans Affairs, Debt Management Center, P.O. Box 11930, St Paul, MN 55111.

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.

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.

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

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

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

Follow the format below:
Privacy Risk: There is a risk that individuals may seek to access or redress records about them held by the VA Office and become frustrated with the results of their attempt.

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 the point of contact for members of the public who have questions or concerns about applications, evidence files, or correction of inaccurate information.

Section 8. Technical Access and Security

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

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

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

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

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

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

All individuals are subject to a background investigation before system access is granted. All individuals with system access are required to complete the VA Privacy and Information Security Awareness and Rules of Behavior training annually.

Salesforce - Veterans Account Management System Debt Management Center (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 duty has been applied as appropriate.

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 may have access to Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC). All contractors sign the VA Rules of Behavior, just as VA Employees do, and they pass a Background Investigation prior to receiving access to Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC).

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 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.

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

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

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

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

If Yes, provide:

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

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

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

1. The Security Plan Status: Not Yet Approved
2. The Assessment Status: Approved
3. The Assessment Date: 26-Jan-2022
4. The Authorization Termination Date: 17-Dec-2023
5. The FIPS 199 classification of the system: Moderate

Note: Since this is a minor application it falls under the eMASS assessment process which differs from the authorization process of a minor application.

Section 9 – Technology Usage

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

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

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

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

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

Cloud technology used: Yes

Cloud Model: Platform as a Service (PaaS)

Platform/Technology used: Salesforce Government Cloud (FedRAMP)

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.

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.

Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC) is not collecting 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.

SORN 88VA244 contains all the details of agreement between Salesforce, Inc. and the VA.

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).

Not Applicable for Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC).

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

Tonya L. Facemire 234776

Digitally signed by Tonya L. Facemire 234776
Date: 2022.07.22 09:30:13 -04'00'

Privacy Officer, Tonya Facemire

JAMES BORING

Digitally signed by JAMES BORING
Date: 2022.07.21 12:49:44 -04'00'

Information System Security Officer, James Boring

Michael S. Domanski 326889

Digitally signed by Michael S. Domanski 326889
Date: 2022.07.20 13:38:08 -04'00'

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). Privacy, Policies, And Legal Information | Veterans Affairs