Privacy Impact Assessment for the VA IT System called:

Centralized Accounts Receivable System /Centralized Accounts Receivable On-Line (CAO)

VA Central Office

Debt Management Center

Date PIA submitted for review:

02/21/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Morgen Egesdal	Morgen.egesdal@va.gov	612-725-4353
Information System Security Officer (ISSO)	Andrew Longtine	Andrew.longtine@va.gov	320-333-2017
Information System Owner	Joseph Veit	Joseph.Veit@va.gov	612-876-3513

Abstract

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

Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line (CAO) is used to collect and maintain information on individuals that have an accounts receivable resulting from participating in a VA benefit program. It is designed to assist in the collection of government over-payments. CAO reflects the accounts receivable under the jurisdiction of the VA Debt Management Center (DMC). CAO displays debts which are generated from four main Veterans Benefits Administration (VBA) areas: Education, Compensation, Pension and Loan Guaranty. CAO also houses some debts relating to Veterans Health Administration (VHA). CAO is accessed from within VA.gov and not accessible externally.

Overview

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

1 General Description

A. The IT system name and the name of the program office that owns the IT system.

Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line (CAO) belongs to Debt Management Center (DMC) under VA Central Office (VACO)

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

CAO is a mixed legacy and modernized system used to collect and maintain information on individuals that have an accounts receivables resulting from participating in a VA benefit program. CAO is designed to assist in the collection of government over-payments and to provide the DMC and VACO with reports and statistical data on the volume and characteristics of the over-payments.

C. Indicate the ownership or control of the IT system or project.

DMC/ VACO

2. Information Collection and Sharing

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

In order to help fulfill its responsibilities, the St. Paul DMC currently uses a general support system (GSS) to assist in serving 1,000,000 to 9,999,999 veterans and their dependents.

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

Personally identifiable information maintained in the system is used for purposes of collecting the receivables. The CAO system is a web enhanced architecture where the application server, primary external interfaces, and databases are located at the Austin Automation Center, Austin, TX. Users access the system via VA connected workstations. CARS is maintained on the Austin Information Technology Center's mainframe in Austin, TX. The system automatically generates collection notices and stores payment information as well as other data pertinent to the collection process. Updates are sent from CAO to VBA daily for the purpose of updating balances. CAROLS is the CAO web based on-line interface used to view and update the CARS Master Record. The backend of CAROLS is a SQL server database that contains limited data fields from the CARS Master Record that displays collection and account information. DMC employees access CAROLS via the web browser and to access records and input updates to CAROLS daily, those updates are processed in CARS every night and CAROLS is then updated from CARS with the most current data.

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

CAO receives updates on a cyclical basis to establish, increase, reduce or delete accounts receivable balances from VBA's Financial Accounting System (FAS) and the Benefit Delivery Network (BDN), as well as input from VHA's VISTA system.

G. 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.

The GSS consists of file servers, routers, printers, and networked PCs which allow for the processing and storage of data necessary for carrying out DMC functions. The St. Paul DMC GSS does not directly host or maintain any major VA systems or applications. Any data stored on the system is the result of employees directly storing or maintaining data, such as Excel Spreadsheets or Word Documents on the network. Although most veteran data is stored in a central database not located at this facility, during the processing of debt, it is often necessary for employees to store files containing personal information on the network. This is done for a variety of reasons to include but not limited to temporary storage while working a case, for reference purposes, or to assist in case management.

3. Legal Authority and SORN

H. A citation of the legal authority to operate the IT system.

Generally, the 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; PL 94-466, The Veterans Rehabilitation and Education Amendments of 1980 as amended: The Debt Collection Act of 1982 (PL97-365). Specific authority to operate the St. Paul General Support System (GSS) from which the DMC accesses the VA network is Title 10 U.S.C. chapters 106a, 510, 1606 and 1607 and Title 38, U.S.C., section 501(a) and Chapters 11, 13, 15, 18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51, 53, and 55. SORN 88VA244 Central Accounts Receivable System/Centralized Accounts Receivable On-Line System https://www.govinfo.gov/content/pkg/FR-2018-08-13/pdf/2018-17228.pdf.

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

The SORN does not currently require amendment.

D. System Changes

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

Not anticipated.

K. *Whether the completion of this PIA could potentially result in technology changes*

Not anticipated.

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 Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers*
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☐ Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☐ Gender
- ☐ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Data Elements (list below)

VA Benefit Overpayment Information

PII Mapping of Components (Servers/Database)

CAO consists of 8 key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by CAO 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 the server names in the table.
The first table of 3.9 in the PTA should be used to answer this question.

Internal Database Connections

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
CAROLS Database	Yes	Yes	Name, Social Security Number, Address, Phone Number, Email Address, Financial Account Info	PII is required for proper identification and processing of Veteran files	Encryption
CarZ Database	Yes	Yes	Name, Social Security Number, Address, Phone Number, Email Address, Financial Account Info	PII is required for proper identification and processing of Veteran files	Encryption
CRS Database	Yes	Yes	Name, Social Security Number, Address, Phone Number, Email Address, Financial Account Info	PII is required for proper identification and processing of Veteran files	Encryption
HRV/IMDB/MDM database	Yes	Yes	Name, Social Security Number, Address, Phone Number, Email Address, Financial Account Info	PII is required for proper identification and processing of Veteran files	Encryption
ODS Database	Yes	Yes	Name, Social Security Number, Address, Phone Number, Email Address, Financial Account Info	PII is required for proper identification and processing of Veteran files	Encryption
Aperta Database	Yes	Yes	Name, Social Security Number, Address, Phone Number, Email Address, Financial Account Info	PII is required for proper identification and processing of Veteran files	Encryption
HDA Database	Yes	Yes	Name, Social Security Number, Address, Phone Number, Email Address, Financial Account Info	PII is required for proper identification and processing of Veteran files	Encryption

HDR Database	Yes	Yes	Name, Social Security Number, Address, Phone Number, Email Address, Financial Account Info	PII is required for proper identification and processing of Veteran files	Encryption

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

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

Sources of data may come from VBA Loan Guaranty Home, Condominium and Manufactured Home Loan Applicant Records; VA, Veterans and Benefits Identification and Location Records; Compensation, Pension, Education and Rehabilitation via BDN database

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.

CAO receives updates on a cyclical basis to establish, increase, reduce or delete accounts receivable balances.

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

VBA Loan Guaranty Home, Condominium and Manufactured Home Loan Applicant Records; VA, Veterans and Benefits Identification and Location Records; Compensation, Pension, Education and Rehabilitation via BDN database

1.3 How is the information collected?

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

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

Data may be collected by paper submission from the Veteran for payments or waivers or via VA file databases. CAO gathers information from FAS, Benefit Delivery Network and/or VISTA. URL of the associated forms may be downloaded from this site filled in and printed to be delivered in paper form

https://www.va.gov/resources/va-debt-management/. All collected information is used to determine eligibility for benefits, process ratings and to provide payments via the Department of Treasury.

1.3b 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.

OMB 2900-0165, VA 5655

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

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

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

All data are matched against supporting claims documentation submitted by the veteran, widow, or dependent. Certain data such as SSN is verified with the Social Security Administration. Prior to any award or entitlement authorization(s) by the VBA, the veteran record is manually reviewed, and data validated to ensure correct entitlement has been approved. Close coordination with the VBA Veteran Service Center (VSC), Pension Management Center (PMC), and other VBA and VHA entities is part of the DMC's standard operating procedure.

1.4b 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.

N/A

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

SORN 88VA244 Central Accounts Receivable System/Centralized Accounts Receivable On-Line System https://www.govinfo.gov/content/pkg/FR-2018-08-13/pdf/2018-17228.pdf. Specific authority to operate the St. Paul General Support System (GSS) from which the DMC accesses the VA network is Title 10

U.S.C. chapters 106a, 510, 1606 and 1607 and Title 38, U.S.C., section 501(a) and Chapters 11, 13, 15, 18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51, 53, and 55

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: Sensitive Personal Information including personal contact information, service information and benefit information may be released to unauthorized individuals.

Mitigation: DMC adheres to the information security requirements instituted by the VA Office of Information Technology (OIT).
•All employees with access to Veteran's information are required to complete the web-based VA Privacy and Information Security Awareness training and Rules of Behavior annually, and upon committing a privacy incident.
•Usage of the Microsoft Outlook setting to encrypt email messages containing PII/PHI/SPI is required of all users.

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 a Veteran Identifier
- Social Security Number: Used as a Veteran Identifier
- Address: Used to contact the individual
- Email Address: Used to contact the individual
- Financial/Payment Information: Used to identify, reference, and maintain benefit overpayments owed
- Benefit Overpayment Information

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

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

The CAO automatically generates collection notices and stores payment information as well as other data pertinent to the collection process. Updates are sent from CARS to FAS/BDN/VISTA daily for the purpose of updating balances. CAROLS is web based on-line interface used to view and update the CARS Master Record database. The backend of CAROLS is a SQL server database that contains limited data fields from the CARS Master Record that displays collection and account information. DMC employees access CAROLS via the web browser and to access records and input updates to CAROLS daily, those updates are processed in CARS every night and CAROLS is then updated from CARS with the most current data.

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.

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 and printed on paper and mailed to the Veteran.

2.3 How is the information in the system secured?

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

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

PII not limited to but including SSN's are protected with FIPS 140-2 encryption at rest and transmission. Supervisory assignment of functional categories restricting employee access to systems information.

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

PII not limited to but including SSN's are protected with FIPS 140-2 encryption at rest and transmission. Supervisory assignment of functional categories restricting employee access to systems information.

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

PII not limited to but including SSN's are protected with FIPS 140-2 encryption at rest and transmission. Supervisory assignment of functional categories restricting employee access to systems information.

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?

As system access is required as a condition of employment for St. Paul 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 or will receive an access denied error.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented?

Yes, DMC uses the VA CRISP initiative for access and has the procedures, controls, and responsibilities documented.

2.4c Does access require manager approval?

Granting of access to CAO requires a request from a SSOD analyst and approval by an Approving Official, and Director in order to be implemented via CSEM.

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

DMC's ISSO records, tracks, and monitors access to PII within CAO for improper access to PII. When improper access is noted, an investigation may take place.

2.4e Who is responsible for assuring safeguards for the PII?
All DMC employees have a responsibility to safeguard the privacy of Veterans and beneficiaries, and to ensure sensitive information remains protected. This responsibility extends to DMC Contractors and trainees.

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 PII to include name, address, and social security number is retained.

3.2 How long is information retained?

In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. ***For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods****. The VA records officer should be consulted*

early in the development process to ensure that appropriate retention and destruction schedules are implemented. If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.

Data is retained for 25 years. Microfilm and microfiche that contain historic information, CARS master record and Hines audit trail have a retention period of 25 years. Due to the nature of Veteran receivables, copies of this information are required for audit purposes. We can terminate collection action and write-off a debt, and then reestablish it years later for offset purposes if the individual becomes entitled to VA benefits. Paper copies of correspondence or related documentation are scanned into an imaging system and are shredded after we verify the images are readable and are correctly indexed into the system.

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

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

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

These records are retained and disposed of in accordance with the General Records Schedule 20, approved by National Archives and Records Administration (NARA).
https://www.archives.gov/records-mgmt/grs.html

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

These records are retained and disposed of in accordance with the General Records Schedule 20, approved by National Archives and Records Administration (NARA).
https://www.archives.gov/records-mgmt/grs.html

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.

Data is shredded at the end of the retention period by a certified contractor. Data retention procedures are enforced by supervisors. Paper and electronic media records that have reached their retention period and are eligible for destruction are shredded on site by Shred-It Inc. which is a national company under VA contract. The destruction process is witnessed by a Records Officer and a certificate of destruction is provided do document the process. Paper media is then shipped to a pulping mill for final destruction where paper is made into various corrugated or wall board material. Electronic media in various forms is first shredded and the recycled. 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 the Department of Veterans' Affairs Directive 6500, VA Cybersecurity Program (February 24, 2021), paragraph 2.b.(5) Media Sanitization. Magnetic media is wiped and sent out for destruction per VA Directive 6500. Digital media is shredded or sent out for destruction per VA Directive 6500. Additionally, CAO follows Field Security Service (FSS) Bulletin 209.1 dated March 18, 2019 for National Media Sanitization and Destruction Program as well as the Development, Security, and Operations (DevSecOps), End User Operations (EUO), Enter Standard Operating Procedures (SOP), Data and Media Protection. All other automated storage media are retained and disposed of in accordance with disposition authorization approved by NARA.

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.

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

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

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

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

<u>Principle of Minimization:</u> 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?

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

Follow the format below:

Privacy Risk: There is a risk that the information maintained by CAO could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation: To mitigate the risk posed by information retention, the CAO adheres to the VA Records Control Schedule 20 schedules for each category or data it maintains. When the retention data is reached for a record, the medical center will carefully dispose of the data by the determined method as described in question 3.4. SSO Records Management, VBA Directive 6300 signed 09/21/18.

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***
Veterans Benefits Administration (VBA)	To obtain payment for a debt created using Veterans Administration benefits	Personally Identifiable Information (PII) to include Name, Social Security Number, Address, Phone Number, Email Address, Financial Account Information	Electronic transmission methods in CARS/CAROLS in accordance with VA policy. Paper records are shared with the VBA to determine debt amounts and collection procedures. Information is electronically transmitted via the SHARE application.
Veterans Health Administration (VHA)	To obtain payment for a debt created using Veterans Administration benefits; Data sent to Office of Mental Health and Suicide Prevention (OMHSP) for the purpose of alerting mental health providers of economic stressors.	Personally Identifiable Information (PII) to include Name, Social Security Number, Address, Phone Number, Email Address, Financial Account Information and Protected Health Information (PHI), appropriate to the agreements	Electronically pulled from VistA thru Computerized Patient Record System (CPRS); Electronic transmission methods between CARS/CAROLS and VHA OMHSP in accordance with VA policy
VBA Benefit Delivery Network (BDN)/VETSNET/VBMS (VBA)	To obtain payment for a debt created using Veterans	Personally Identifiable Information (PII) to include Name, Social Security Number, Address, Phone	This indicates that CAO Processing and receiving PII information for and back from

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*
	Administration benefits	Number, Email Address, Financial Account Information	BDN/VETSNET (VETSNET)/Veterans Benefits
VA Capital Region Readiness Center (CRRC)/Enterprise Web Infrastructure Support (EWIS) (PayVA)	To obtain payment for a debt created using Veterans Administration benefits	Personally Identifiable Information (PII) to include Name, Social Security Number, Address, Phone Number, Email Address, Financial Account Information	Electronic transmission methods in CARS/CAROLS in accordance with VA policy
Veterans Account Management System (VAMS) hosted on Salesforce Government Cloud Assessing (VAMS Salesforce)	Case Management tool used to access veteran account information	Personally Identifiable Information (PII) to include Name, Social Security Number, Address, Phone Number, Email Address, Financial Account Information	Electronic transmission methods in CARS/CAROLS in accordance with VA policy.
VA MuleSoft Cloud Enterprise (MuleSoft-e)	To obtain payment for a debt created using Veterans Administration benefits	Personally Identifiable Information (PII) to include Name, Social Security Number, Address, Phone Number, Email Address, Financial Account Information	Electronic transmission methods in CARS/CAROLS in accordance with VA policy.
Digital Veterans Platform (DVP) Veterans-Facing Services Platform-VA.gov (VFSP-VA.gov)	To obtain payment for a debt created using Veterans Administration benefits	Personally Identifiable Information (PII) to include Name, Social Security Number, Address, Phone Number, Email Address, Financial Account Information	Electronic transmission methods in CARS/CAROLS in accordance with VA policy.

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: 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.

Electronic Permission Access System (ePAS) mitigates the risk of inadvertently sharing or disclosing information by assigning access permissions based on need to know.

The use of a Personal Identity Verification (PIV) card is implemented. This ensures the identity of the user by requiring two-factor authentication.

Microsoft Outlook is also another tool that is used to share internal information within the organization. Risks are mitigated by using encryption methods to share sensitive information within the organization.

Section 5. External Sharing/Receiving and Disclosure

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

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

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

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

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
Credit Reporting Agencies (Equifax, Experian, Innovis, TransUnion)	To obtain payment for a debt created using Veterans Administration benefits	SSN, Name, Address, Phone Number, debt information	MOU/ISA	Secure Files Transfer Protocol (SFTP)FTP
Document Security Solutions	PII is shredded by document destruction company	SSN, Name, Address, Phone Number, debt Information	Agreement with Document Security Solutions receipt of certificate of destruction	Data is not transmitted. Paper is shredded on VA facilities grounds according to contract.
US Department of Housing and Urban Development (HUD)	To obtain payment for a debt created using Veterans	SSN, Name, Address, Phone Number, debt Information	MOU/ISA	Secure Files Transfer Protocol (SFTP)

	Administration benefits			
US Department of Treasury Bureau of Fiscal Service	To obtain payment for a debt created using Veterans Administration benefits	SSN, Name, Address, Phone Number, debt Information	MOU/ISA	Direct Connect

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Follow the format below:

Privacy Risk: 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 DMC adheres to all information security requirements instituted by the VA Office of Information Technology (OIT).
•Information is shared in accordance with VA Handbook 6500. There are also system safeguards in place to restrict access to information and data to only those who having a genuine work related need to know. These safeguards are in place in the St. Paul GSS as well as all VA systems.

Although a natural risk of disclosure exists with the sharing of information internally or externally, VA mitigates that risk by creating and maintaining system safeguards which bar access to those who do not have a genuine work-related need for the information/data collected.

Section 6. Notice

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

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

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

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

The Department of Veterans Affairs also provides notice by publishing the VA System of Record Notice (VA SORN) SORN 88VA244 Central Accounts Receivable System/Centralized Accounts Receivable On-Line System (August 13, 2018) , in 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 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." (Reference Appendix 1)

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

N/A

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

The Department of Veterans Affairs also provides notice by publishing the VA System of Record Notice (VA SORN 88VA244 Central Accounts Receivable System/Centralized Accounts Receivable On-Line System (August 13, 2018) inthe 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.. 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." (Reference Appendix 1)

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

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

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

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

Privacy Risk: 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 3 main forms of notice are discussed in detail in question 6.1 and include the Privacy Act statement, 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?

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

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

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 inwriting 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 inwriting 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 5U.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 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 so 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 determinations 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 hat 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 (5U.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.

7.1b 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).

N/A

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.

N/A

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 88VA244 Central Accounts Receivable System/Centralized Accounts Receivable On-Line System (August 13, 2018),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. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Individuals 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 Regional Office 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://www.benefits.va.gov/ROPHILADELPHIA/index.asp.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that 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 VBMS (Veterans Benefit Management System) Legacy platform. Furthermore, this document and the SORN provide the point of contact for members of the public who have questions or concerns about applications and evidence files.Section 8. Technical Access and Security

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

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

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

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

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.

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?

Access to VBA applications is requested electronically through Common Security Employee Manager and approved by designated Requesting Officials, Station Director (if sensitive level is above 0 is requested), and Information Security Officer.

8.1c Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

VA employees 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. Other users are required to have specific needs and must be verified as having security and privacy training. The access is deleted once the specific needs are completed.

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 will have access to the system upon completion of VA Privacy and Information Security Awareness training, signing VA Rules of Behavior, and successfully completing a background investigation. The contracts are reviewed annually when option years are exercised, and a background investigation is required to access the system. Annual recertification is verified by the station training coordinator, ISSO, Privacy Officer, or Contracting Officer.

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 station employees are provided initial training within the first week of employment on how to use the GSS system to include training on how to ensure that information security is maintained. Additionally, employees are given a minimum of five hours of annual refresher training on information security, as well as a refresher on rules and behaviors related to use of VA electronic equipment. All Station/VA employees who have access to VA computers must complete the onboarding and annual mandatory privacy and information security training. In addition, all employees who interact with patient sensitive medical information must complete the VA mandated privacy HIPAA training. Finally, all new employees receive face-to-face training by the St. Paul VA Medical Center Privacy Officer and Information Security Officer during new employee orientation. The Privacy and Information Security Officer also perform subject specific trainings on an as needed basis. Additionally, employees are given a minimum of five hours of annual refresher training on information security, as well as a refresher on rules and behaviors related to use of VA electronic equipment.

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

8.4a If Yes, provide:

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

The Authorization and Accreditation (A&A) for Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line (CAO) is as follows: System Security Plan Approved 06/15/2021; Authorization Status is three-year Authorization to Operate (ATO) on 08/03/2021 with an Authorization Termination Date (ATD) of 08/02/2024; Risk Assessment was completed 09/09/2021; The FIPS 199 classification is MODERATE. *Please note that all systems containing SPI are categorized at a minimum level of "moderate" under Federal Information Processing Standards Publication 199.*

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***

Please provide response here

Section 9 – Technology Usage

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

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

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

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

CAO connects to a hybrid cloud solution with MulesSoft. MuleSoft is a separate system and platform. MuleSoft is a middleware integration platform. It does not contain a data repository to persist PII or business data at rest. No data is stored.

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

N/A

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.

N/A

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.

N/A

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).

N/A

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

ID	Privacy Controls
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.

Morgen M. Egesdal 1363423

Digitally signed by Morgen M. Egesdal 1363423
Date: 2023.03.03 12:46:20 -06'00'

Privacy Officer, Morgen Egesdal

ANDREW LONGTINE

Digitally signed by ANDREW LONGTINE
Date: 2023.03.03 13:50:24 -06'00'

Information System Security Officer, Andrew Longtine

JOSEPH VEIT

Digitally signed by JOSEPH VEIT
Date: 2023.03.08 07:45:59 -06'00'

Information System Owner, Joseph Veit

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).

HELPFUL LINKS:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

VA Privacy Service Privacy Hub:

https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices