Privacy Impact Assessment for the VA IT System called:

PayVA

Veterans Administrations Central Office (VACO)

Debt Management Center; Maintained by VA Capital Region Readiness Center (CRRC)/Enterprise Web Infrastructure Support (EWIS)

Date PIA submitted for review:

08/14/2023

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)	James Weinhold	James.Weinhold@va.gov	612-946-4428
Information System Owner	Karen L. Kelly	Karen.Kelly1@va.gov	202-876-7958

Abstract

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

PayVA is a custom-developed application (which is a website; https://www.pay.va.gov) that is used by the Debt Management Center (DMC) to verify debts are active at DMC before the Veteran makes a payment. PayVA collects basic debt information from users, redirects them to pay.gov (Department of Treasury) for online payments and collects responses from pay.gov. The Veteran enters their personal information to include File Number, Payee Number, Deduction Code, First Name, Last Name, Phone Number, and Payment Amount. VA DMC and Information Technology employees access the system through an internal administrative console using Single Sign-On (SSOi). The production site with a secure certificate has already been created.

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.

PayVA, Debt Management Center: maintained by the VA Capital Region Readiness Center (CRRC)/Enterprise Web Infrastructure Support (EWIS)

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

Verification of active debts of veterans with the debt management center.

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

VA Owned and VA Operated Debt Management Center, maintained by the VA Capital Region Readiness Center (CRRC)/Enterprise Web Infrastructure Support (EWIS)

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.

100,000+ veterans with an active debt.

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

PayVA is a custom-developed application (which is a website; https://www.pay.va.gov) that is used by the Debt Management Center (DMC) to verify debts are active at DMC before

the Veteran makes a payment. PayVA collects basic debt information from users, redirects them to pay.gov (Department of Treasury) for online payments and collects responses from pay.gov. The Veteran enters their personal information to include File Number, Payee Number, Deduction Code, First Name, Last Name, Phone Number, and Payment Amount. VA DMC and Information Technology employees access the system through an internal administrative console using Single Sign-On (SSOi). The production site with a secure certificate has already been created. PayVA is housed in the WebOps server farm at the Capital Region Readiness Center (CRRC) in Martinsburg, WV. The system purpose is verification of active debts of veterans with the debt management center, and provide a portal for payment of debts to the Department of Treasury (Pay.gov)

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

PayVA receives information (a table containing PII) from the Centralized Accounts Receivable System /Central Accounts Receivable On-Line System (CARS/CAROLS) an internal VA system, via a SQL job 3 times a week. PayVA also receives information each time a payment is completed via a form submission from Pay.Gov which is owned by the Department of Treasury.

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.

PayVA is operated at one site, the Capital Region Readiness Center, (CRRC)

3. Legal Authority and SORN

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

Title 10 United States Code (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. PayVA SORN 194VA189 (https://www.oprm.va.gov/privacy/systems_of_records.aspx

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

No.

D. System Changes

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

No

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

No

Section 1. Characterization of the Information

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

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

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

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

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

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)

File Number (which is sometimes the SSN and sometimes the SSN, reformatted); Payee Number; Deduction Code (which can be found in a letter the user received from the DMC), Person entitled (Payee) and Payment amount. PayVA then verifies the information entered by the user against a

table provided by CARS/CAROLS (an internal VA system). If the information entered is correct the user is directed to the Department of Treasury's Pay.Gov where payment is made, and then a form submission with the user's partial bank account number/credit card number and payer name is provided to PayVA and stored in its database.

PII Mapping of Components (Servers/Database)

PayVA consists of 1 key component (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by PayVA 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
payva_restore data	**Yes**	**Yes**	File Number (SSN), Payee Number, First Name, Last Name, Phone Number, and Payment Amount	SSN is required for proper identification of veteran.	**Encryption (SSL/HTTPS)**

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?

PayVA receives the following information from the user, directly, First Name, Last Name, Daytime Phone, File Number, Payee Number, Person Entitled, Deduction Code, and Payment Amount. PayVA, then checks whether the information entered by the user matches what is in the CARS/CAROLS table that is received by PayVA, 3 times a week; each time the table is refreshed the former table is deleted (no historical data from CARS/CAROLS is stored in PayVA). If the information entered by the User matches what is in the table received from CARS/CAROLS the user is transferred to Pay.Gov (which is managed by the Department of Treasury), where the payment is made. The only information PayVA shares with Pay.Gov is the first name, last name, and debt

amount. The user then enters the following information to Pay.Gov, the Payment Amount, Account Type, Routing Number, and Account Number (which would be covered by the Department of Treasury's accreditation documentation). Once the payment is completed Pay.Gov passes payment results including partial bank account number, credit card number, and payer name which is stored in PayVA's 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.

CARS/CAROLS is a VA internal application, the data elements of which are used only to verify that the information the user enters is accurate.

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

The system does not create any information such as a score, analysis, or report.

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?

PayVA first receives information directly from the user. The user must go to https://www.pay.va.gov and select, "Pay Online," then they will be taken to a new screen where they will populate their First Name, Last Name, Daytime Phone, File Number, Payee Number, Person Entitled, Deduction Code, and Payment Amount. The information entered is then checked against a table provided by CAROLS 3 times a week via a SQL job.

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.

Information is collected through the web portal. OMB Number: 2900-0663 Estimated Burden: 10 minutes

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.

PayVA checks for accuracy immediately. If the information entered by the user does not match the information PayVA receives from CARS, the user gets the following message and is not able to proceed with the payment: "Please call the Debt Management Center at 1-800-827-0648 before proceeding with this payment on Pay.gov."

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.

Commercial aggregation sources are not used to check the data for accuracy.

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

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

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 10 United States Code (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 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>

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:

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

<u>Principle of Minimization:</u> 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) and stores the name, partial bank account number, and sometimes the SSN (if used as the File Number). Due to the 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 the information is not disclosed or released. Safeguards and security controls are in place (to include access control, security awareness training, and audit and accountability). PayVA is a VA managed application which 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.

Name – Used as identifier.
SSN – Sometimes used as the File Name which is used as an identifier.
Payee Number – Used as identifier.
Deduction Code – Used as identifier.
Financial Account Information –Used as identifier and proof of payment.

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.

PayVA data is entered by the user, and then is checked against data (a table provided via a SQL job 3 times a week by another internal VA system, CARS/CAROLS). PayVA only keeps the most recent table provided by CARS/CAROLS; (information regarding records for CARS/CAROLS files can be found in the CARS/CAROLS PIA). Once the data entered by the user is checked against the CARS/CAROLS table and/if the information matches, the user is directed to Pay.Gov (owned by the Department of Treasury) where the payment is made. At that time, Pay.gov provides the payment results, including partial bank account number/credit card number and payee name to PayVA and that information is stored in the PayVA database indefinitely.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

The system neither creates, nor makes available new or previously unutilized information about an individual. A new record is created by Pay.gov (Department of Treasury) which is the payment transaction record, which includes the payee name and partial bank account/credit card number, and is stored in the PayVA database for financial audit purposes.

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?

All information of data in transit uses Secure Socket Layers/Transport Layer Security over Hypertext Transfer Protocol (HTTPS). Data at rest is protected on the Storage Area Network (SAN) through ONTAP Internetwork Operating System (iOS), which is a fully FIPS 140-2, level 1 encryption compliant and meets the VA6500 requirements for data at rest encryption.

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

All information of data in transit uses Secure Socket Layers/Transport Layer Security over Hypertext Transfer Protocol (HTTPS). Data at rest is protected on the Storage Area Network (SAN) through

ONTAP Internetwork Operating System (iOS), which is a fully FIPS 140-2, level 1 encryption compliant and meets the VA6500 requirements for data at rest encryption.

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

VA employees and contractors are required to take annual privacy training through the VA's Training Management System (TMS) and sign Rules of Behavior. Any employee or contractor who fails to recertify annually will have their VA network and application access suspended until they are in compliance with the requirement. VA employees and contractors are required to report all incidences of suspected or actual PII disclosure to a VA Information System Security Officer (ISSO) within one hour of discovering the incident. VA Handbook 6500.2, dated June 30, 2023, is the enterprise-wide Privacy Incident Response Plan. Privacy Service, OIT and Data Breach Response Service (DBRS) are responsible for implementation of VA Handbook 6500.2 as well as Privacy incident response plan procedures, including investigation and extra-agency reporting.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

All system administrators granted access to VA systems are given access based on their position, duties and a job related need to know. All system administrators are also required to have extensive training prior to receiving access and are required to recertify and resign the VA Rules of Behavior, annually, or lose their access to the VA network and applications until they are in compliance with the training requirements. System Administrator access is granted via ePAS.

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

Supervisory approval for system administrators is documented in ePAS. Required Privacy and Security Training is documented in the VA Training Management System.

2.4c Does access require manager approval?

All system administrators granted access to VA systems are given access based on their position, duties and a job related need to know, and requires management approval. All system administrators are also required to have extensive training prior to receiving access and are required to recertify and resign the VA Rules of Behavior, annually. System Administrator access is granted via ePAS, and requires management approval. End Users of PayVA must have a copy of the letter sent to the debtor by the Debt Management Center (DMC) to utilize the system which is used to verify the user's identity. They must then enter the information found in the upper right-hand corner of the letter from DMC. The debtor must then enter the same information found in the letter in lines 2 through 4 on the PayVA webpage. If the data entered by the user does not match, the debtor is not able to move forward with the payment and gets the following message: "Please call the Debt Management Center at 1-800-827-0648 before proceeding with this payment on Pay.gov."

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

Administrative access and actions are logged in the VA's system and application log aggregation system, SPLUNK. Activity Reports may be run on an ad-hoc basis.

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

PayVA and DMC employ an Information System Security Officer (ISSO) whose primary duty is to monitor sensitivity levels assigned to PayVA and 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*

Payment results are provided by Pay.Gov (system owned by the Department of Treasury) upon payment completion. The payment results contain the following PII which is stored indefinitely in PayVA's Database is: partial bank account number/credit card number, and the payer name. PayVA also receives a table from CARS/CAROLS (an internal system to VA) 3 times a week via a SQL job that contains the following PII, File Number (which is sometimes the SSN), Payee Number and Deduction Code.

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.*

These records are retained and disposed of in accordance with the General Records Schedule 3.1 010-020, approved by National Archives and Records Administration (NARA) https://www.archives.gov/files/records-mgmt/grs/grs03-1.pdf. A retention policy specific to PayVA is being drafted. This PIA will be updated with that information upon completion; until that time, PayVA is retaining all records indefinitely.

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

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

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

Yes - These records are retained and disposed of in accordance with the General Records Schedule 1.1 010-011 and 3.1 010-020, approved by National Archives and Records Administration (NARA) https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf and https://www.archives.gov/files/records-mgmt/grs/grs03-1.pdf.

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

General Records Schedule 1.1 010-011 - DAA-GRS2013-0003-0001, DAA-GRS2013-0003-0002 and General Records Schedule 3.1 010-020 - DAA-GRS2013-0005-0006, DAA-GRS2013-0005-0007, DAA-GRS2013-0005-0008, DAA-GRS2013-0005-0009.
https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

3.4 What are the procedures for the elimination or transfer of SPI?

Explain how records are destroyed, eliminated or transferred to NARA at the end of their mandatory retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.? This question is related to privacy control DM-2, Data Retention and Disposal.

Financial transaction records related to … collecting debts (GRS 1.1 010, 11): Destroy 6 years after final payment or cancellation, but longer retention is authorized if required for business use. Destroy when business use ceases. Project Records (3.1 010, 011): Destroy 5 years after project is terminated, but longer retention is authorized if required for business use. Special Purpose Programs and Applications (3.1 012): Delete when related master file or database has been deleted, but longer retention is authorized if required for business use. Information Technology Records (3.1 020): Destroy 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated, or superseded, but longer retention is authorized if required for business use. PayVA adheres to VA Directive 6500, VA Cybersecurity Program, and VA Handbook 6500.2, Management of Breaches Involving Sensitive Personal Information, among other VA directives, to manage the protection of, and minimize the usage of, sensitive personal information (SPI).

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. Risk minimization includes data obfuscation (use of partial PII), use of stale data, or use of anonymized data. Any use of data that may include PII must be documented and approved for use by VA leadership in accordance with VA Handbook 6502, VA Enterprise Privacy Program and VA Handbook 6508.1, Procedures for Privacy Threshold Analysis and Privacy Impact Assessment.

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:

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. These records are retained and disposed of in accordance with the General Records Schedule 3.1 010-020, approved by National Archives and Records Administration (NARA) https://www.archives.gov/records-mgmt/grs.html. A retention policy specific to PayVA is being drafted This PIA will be updated with that information upon completion; until that time, PayVA is retaining all records indefinitely.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Central Accounts Receivable System/Centralized Accounts Receivable On-Line System (CARS/CAROLS)	To ensure the payment is allotted to the correct debt/debtor	File Number which is the SSN for newer debts and is the SSN (but reformatted) for older debts.	SQL JOB (3 times a week

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 by authorized users.

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 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***
Department of Treasury (PayVA.gov)	To ensure record of payment by the Veteran.	SSN (File number), Name, Amount of payment	SORN 194VA189. Agency Participation Agreement	Open Collections Interface (OCI)

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: There is a risk that data could be shared with an inappropriate and/or unauthorized external organization or institution.

Mitigation: The safeguards implemented to ensure data is not shared with the wrong external organization are use of secure data transfer protocols and encryption (Secure Socket Layers/Transport Layer Security over Hypertext Transfer Protocol (HTTPS).

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.

At U.S. Department of Veterans Affairs - Pay Online (va.gov), A Privacy Notice is available for the user to click on via a link entitled, "Read Important Privacy Information." A copy of the Privacy Information is included as Appendix A. The legal authorities are provided in the first paragraph of the PayVA Privacy Information (38.U.S.C.5701; Privacy Act of 1974; The PayVA SORN is 194VA189. SORNs 58VA21/22 Compensation, Pension, Education and Rehabilitation Records-VA, and 88VA244, Accounts Receivable Records-VA (as can be seen below and in Appendix A)."Privacy Act Information: The information you furnish on this form, including your Social Security Number, is used to associate your payment with your accounts receivable record so that we may properly credit your account. Disclosure is voluntary. However, without disclosure, a credit card transaction or direct debit transaction cannot be processed. The responses you submit are confidential and protected from unauthorized disclosure by 38 U.S.C. 5701. The information may be disclosed outside the Department of Veterans Affairs (VA) only when authorized by the Privacy Act of 1974, as amended. The routine uses for which VA may disclose the information can be found in VA systems of records, including 58VA21/22, Compensation, Pension, Education and Rehabilitation Records-VA, and 88VA244, Accounts Receivable Records-VA. VA systems of records and alterations to the systems are published in the Federal Register. Any information provided by you, including your Social Security Number, may be used in computer matching programs conducted in connection with any proceeding for the collection of an amount owed by virtue of your participation in any benefit program administered by VA."

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.
Notice is provided at https://www.pay.va.gov/index.cfm?action=step1

"Privacy Act Information: The information you furnish on this form, including your Social Security Number, is used to associate your payment with your accounts receivable record so that we may properly credit your account. Disclosure is voluntary. However, without disclosure, a credit card

transaction or direct debit transaction cannot be processed. The responses you submit are confidential and protected from unauthorized disclosure by 38 U.S.C. 5701. The information may be disclosed outside the Department of Veterans Affairs (VA) only when authorized by the Privacy Act of 1974, as amended. The routine uses for which VA may disclose the information can be found in VA systems of records, including 58VA21/22, Compensation, Pension, Education and Rehabilitation Records-VA, and 88VA244, Accounts Receivable Records-VA. VA systems of records and alterations to the systems are published in the Federal Register. Any information provided by you, including your Social Security Number, may be used in computer matching programs conducted in connection with any proceeding for the collection of an amount owed by virtue of your participation in any benefit program administered by VA."

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 notice provided has been vetted by VA Chief Privacy Officer as being in compliance with Federal and VA requirements for disclosure of information collection to the public/end user.

Notice is provided at https://www.pay.va.gov/index.cfm?action=step1

"Privacy Act Information: The information you furnish on this form, including your Social Security Number, is used to associate your payment with your accounts receivable record so that we may properly credit your account. Disclosure is voluntary. However, without disclosure, a credit card transaction or direct debit transaction cannot be processed. The responses you submit are confidential and protected from unauthorized disclosure by 38 U.S.C. 5701. The information may be disclosed outside the Department of Veterans Affairs (VA) only when authorized by the Privacy Act of 1974, as amended. The routine uses for which VA may disclose the information can be found in VA systems of records, including 58VA21/22, Compensation, Pension, Education and Rehabilitation Records-VA, and 88VA244, Accounts Receivable Records-VA. VA systems of records and alterations to the systems are published in the Federal Register. Any information provided by you, including your Social Security Number, may be used in computer matching programs conducted in connection with any proceeding for the collection of an amount owed by virtue of your participation in any benefit program administered by VA."

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.

The individual has the right to decline to provide information; however, on-line payment cannot be processed if the individual refuses to provide information as is stated in the PayVA Privacy Information link; "Privacy Act Information: The information you furnish on this form, including your Social Security Number, is used to associate your payment with your accounts receivable record so that we may properly credit your account. Disclosure is voluntary. However, without disclosure, a credit card transaction or direct debit transaction cannot be processed. The responses you submit are confidential and protected from unauthorized disclosure by 38 U.S.C. 5701."

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.

The individual consents to an overall usage of their information by choosing to proceed with the on-line payment as is stated in the Privacy Information link. "Privacy Act Information: The information you furnish on this form, including your Social Security Number, is used to associate your payment with your accounts receivable record so that we may properly credit your account. Disclosure is voluntary. However, without disclosure, a credit card transaction or direct debit transaction cannot be processed. The responses you submit are confidential and protected from unauthorized disclosure by 38 U.S.C. 5701."

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: The user may choose not to read the link that discusses the Privacy Information for PayVA.

Mitigation: The user is told in a Warning (without having to select the Privacy Information link, "This U.S. Government computer system is for official use only. The files on this system include Federal records that contain sensitive information. All activities on this system may be monitored to measure network performance and resource utilization; to detect unauthorized access to or misuse of the system or individual files and utilities on the system, including personal use; and to protect the operational integrity of the system. Further use of this system constitutes your consent to such monitoring. Misuse of or unauthorized access to this system may result in criminal prosecution and disciplinary, adverse, or other appropriate action."

Section 7. Access, Redress, and Correction

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

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

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

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

Individuals cannot access their information in PayVA. It is simply a place to submit their information. PayVA is used to verify the amount of debt prior to payment to Department of Treasury's Pay.Gov. This can be found on the PayVA website. "If you have comments regarding this burden estimate or any other aspect of this collection of information, contact: U.S. Department of Veterans Affairs Debt Management Center P.O. Box 11930 Ft. Snelling, MN 55111 1-800-827-0648 (Toll Free) 612-970-5688 (fax)"

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).

The system is not exempt from the access provisions of the Privacy Act.

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.

The system is a privacy act system.

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

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

If inaccurate information is provided by the user on the PayVA website, the user is not able to move forward with payment and the following message is received: "Please call the Debt Management Center at 1-800-827-0648 before proceeding with this payment on Pay.gov."

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

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

Individuals are told via the PayVA website, "If you have comments regarding this burden estimate or any other aspect of this collection of information, contact : U.S. Department of Veterans Affairs Debt Management Center P.O. Box 11930 Ft. Snelling, MN 55111 1-800-827-0648 (Toll Free) 612-970-5688 (fax)"

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.

The individual must contact the Debt Management Center as is stated on the PayVA website.

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 the user will not enter the correct information from their DMC letter.

Mitigation: The payment will not be able to be processed and they will have to contact the Debt Management Center at 1-800-827-0648 (Toll Free) or 612-970-5688 (fax).

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.

System Administrators are granted access via Electronic Permission Access System (EPAS) which is a VA system that is monitored and audited. Procedure for New Account/ Modification/ Re-activation/ Deactivation of accounts:1) Requestor – submits an ePAS request with all appropriate access noted and routed to Supervisor for approval. The request will be submitted by completing a request through the Infrastructure Operations (IO) ePAS link. 2) For new accounts only a) (Employee) Human Resource Security - validates information for new Full Time Employees (FTE) and routes the request to the Information Security Officer (ISO) for approval. b) (Contractor) Physical Security - validates new contractor employee and routes the request to the ISO for approval.3) ISSO - reviews, validates the request and routes it to Delegate Authority Official (DAO) for verification and approval. If the request is denied, ISSO sends the notification of denial to the requestor.4) Once the DAO approves the request it is automatically routed to the appropriate Administrative group(s) for access to the systems for processing to create/remove accounts. System Administrators will process the ePAS request based on the access requested by the requestor.5) The requestor will receive the notification that the request is completed. Anyone may access the PayVA website, but the user must verify their identity by entering information found in their letter received from the DMC. If the information is entered incorrectly, the user receives the following message,

"Please call the Debt Management Center at 1-800-827-0648 before proceeding with this payment on Pay.gov."

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?

No users from other agencies have access to PayVA.

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.

No users of PayVA have permissions sufficient to change the data served on PayVA.gov.

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 PayVA. All contractors sign the VA Rules of Behavior, just as VA Employees do, and they pass a Background Investigation prior to receiving access to PayVA.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 btained 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?

YES

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 10/17/2022
3. *The Authorization Status:* Authority to Operate (ATO)
4. *The Authorization Date:* 01/09/2023
5. *The Authorization Termination Date:* 01/09/2024
6. *The Risk Review Completion Date:* 09/21/2022
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

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

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)*

The system does not use Cloud technology.

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.*

The system does not use Cloud technology.

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.

The system does not use Cloud technology.

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.

The system does not use Cloud technology.

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).

The system does not use RPA.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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 provided in this Privacy Impact Assessment is true and accurate.

MORGEN EGESDAL

Digitally signed by MORGEN EGESDAL
Date: 2023.08.24 16:30:57 -05'00'

Privacy Officer, Morgen Egesdal

James W Weinhold 3565781

Digitally signed by James W Weinhold 3565781
Date: 2023.08.28 14:16:07 -05'00'

Information Systems Security Officer, James Weinhold

Karen L. Kelly 105014

Digitally signed by Karen L. Kelly 105014
Date: 2023.08.28 16:10:32 -04'00'

Information Systems Owner, Karen L. Kelly

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 Act Information: The information you furnish on this form, including your Social Security Number, is used to associate your payment with your accounts receivable record so that we may properly credit your account. Disclosure is voluntary. However, without disclosure, a credit card transaction or direct debit transaction cannot be processed. The responses you submit are confidential and protected from unauthorized disclosure by 38 U.S.C. 5701. The information may be disclosed outside the Department of Veterans Affairs (VA) only when authorized by the Privacy Act of 1974, as amended. The routine uses for which VA may disclose the information can be found in VA systems of records, including 58VA21/22, Compensation, Pension, Education and Rehabilitation Records-VA, and 88VA244, Accounts Receivable Records-VA. VA systems of records and alterations to the systems are published in the Federal Register. Any information provided by you, including your Social Security Number, may be used in computer matching programs conducted in connection with any proceeding for the collection of an amount owed by virtue of your participation in any benefit program administered by VA."

https://www.pay.va.gov/index.cfm?action=step1

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