Privacy Impact Assessment for the VA IT System called:

VETERANS CANTEEN SERVICE

AUTOMATED INFORMATION SYSTEM (VCS AIS)

VETERANS CANTEEN SERVICE

eMASS ID 130

Date PIA submitted for review:

02/02/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Teresa Jones-Pirtle	teresa.jones pirtle@va.gov	314-845-1332
Information System Security Officer (ISSO)	Wesley Brown	Wesley.Brown6@va.gov	314-894-6468
Information System Owner	Lisa M. Leonelli	Lisa.Leonelli@va.gov	801-588-5214

Abstract

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

Veterans Canteen Service Automated Information System (aka VCS AIS) is a suite of applications used by the Veterans Canteen Service (VCS) that includes the following applications: Automated Sales Reporting System (ASR); Electronic Card System (ECD); Automated Payroll Deduction System (EPD); VCA Web application (VCW); and Retail, Accounting, Procurement, and Technology with Organizational Reporting (RAPTOR).

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. What is the IT system name and the name of the program office that owns the IT system?

The Veterans Canteen Service Automated Information System (VCS AIS) is a suite of applications owned by the Veterans Canteen Service (VCS) program office. It handles the entire VCS operation: Cash Register system, financial, procurement, human resources, payroll deduction and all other VCS operations. Personal Identifiable Information is in the following modules: payroll deduction; treasury offset program and human resource modules. The expected number of individuals that will have their PII stored in this system: 240000. Within this suite of applications, The Electronic Payroll Deduction EPD application basically consists of daily updates from the canteens on individual purchases that are processed in the nightly batch processing cycle and passed to the Human Resources - Payroll Application Services (Cloud) Assessing (HR-PAS) system for deduction from the individual's payroll account every 2 weeks. Data transmissions utilize FIPS 140-2 certified encryption module to protect the confidentiality of the data being transmitted. See Austin Information Technology Center (AITC) Directive 6700, Information Security and AITC Handbook 6700.6, Information Systems and Communication Protection.

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

The ECD application is a reloadable card program each canteen will use to record meals served to students, doctors, volunteers, etc., and provide detailed information for billing purposes to the appropriate parties. The VCS Canteen e-Business Application Suite/Retail Application Programs RAP is Oracle based and used to help manage food and retail procurements, track deliveries, post receipts of merchandise, pay suppliers, track sales history, record and publish financial information and forecast future purchasing requirements. The RAP application provides extensive management support with various reports and includes retail accountability interfaces with the VCS Finance Center. EDI (electronic data interchange) allows VCS purchase orders to be electronically sent to vendors and it allows vendors to electronically send their invoices to VCS and through

Oracle. This enables VCS to automatically reconcile purchase orders, receipts and invoices. VCS uses St Paul Software (SPS) Commerce as its third-party EDI provider.

C. Who is the owner or control of the IT system or project?

VA Owned and VA Operated IS

2. Information Collection and Sharing

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

240000 personnel with EPD accounts to include current and former VA employees, contract workers.

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

The VCS Canteen e-Business Application Suite/Retail Application Programs RAP is Oracle based and used to help manage food and retail procurements, track deliveries, post receipts of merchandise, pay suppliers, track sales history, record and publish financial information and forecast future purchasing requirements.

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

The RAP application provides extensive management support with various reports and includes retail accountability interfaces with the VCS Finance Center. EDI (electronic data interchange) allows VCS purchase orders to be electronically sent from Oracle to vendors and it allows vendors to electronically send their invoices to VCS and through Oracle. This enables VCS to automatically reconcile purchase orders, receipts and invoices. VCS uses SPS Commerce as its third-party EDI provider. VCS staff use a tool called the EDI "preprocessor" to resolve vendor EDI invoices submitted with errors that are essentially rejected by the system. Invoice errors may include incorrect store location, cost, dates, etc. VCS staff notifies the vendor of any errors so they can be reprocessed with the correct information and pass through the system. Purchase Order Management System (POMS) application is used for VCS Special Order to record customer orders and maintain vendor and item information. EPD customer balance information is shared with VCS' cash register system in order to keep account balances current at the cash register and ensure customers have sufficient balances to make purchases VCS AIS. VIS-AIS's Sim module (subsystem for RAP), interface with VCS MDM handheld scanners.

G. Is 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 system is operated across multiple sites and the same controls are utilized across these sites. The information is shared as follows:

• EDI functionality disburses purchase orders from Oracle to SPS Commerce who then transmits the information to applicable suppliers. Information includes store location number and address, purchase order, item number, item description, quantity ordered. Suppliers receive the purchase orders and fulfill, ship the order to canteens for receiving into Oracle Retail Store Inventory Management (SIM) and stock and sell the merchandise.

Suppliers then bill VCS and transmit an invoice. The invoice is sent to SPS Commerce who sends it to Oracle Retail Invoice Matching (REIM) for invoice matching.

• EPD customer balance information is shared with VCS' cash register system in order to keep account balances current at the cash register and ensure customers have sufficient balances to make purchases. There is a separate EPD server in St. Louis, MO where EPD information is passed through from AITC in order to update the cash register balances. EPD transactions are also collected through automated scripts periodically run throughout the day by St. Louis Area and held in their Data Center. These transactions are then transmitted to AITC's EPD database to update customer balances. EPD also shares information with the PAID system, so customer payments are deducted from their payroll account and their EPD account.

• RAP's Oracle SIM module interfaces with Handheld scanners, which are devices used at each canteen location to perform standard operating procedures required by Oracle SIM such as stock counts, receiving, pick lists, etc. It allows users to interface with Oracle SIM while away from their workstation/desktop computer. Data can be uploaded to Oracle SIM either wirelessly or via direct connection to a canteen workstation.

• Register Transaction (RT) Logs are generated from each canteen operation's cash register at the end of day. RT Logs include daily sales information. RT Logs are collected at the individual canteen's canteen workstation (CWS) and then submitted to St. Louis, MO's central cash register server and then transmitted to AITC where the information is posted into Oracle. In order to sell an item on the cash register, the item must be built in Oracle. These items are driven from Oracle to the register via nightly batch processing. Information includes item Oracle Retail Item Number ORIN # or Universal product codes (UPC), description and sell price.

3. Legal Authority and SORN

H. What is the citation of the legal authority to operate the IT system?

Title 38, United States Code, Part V, Chapter 78, and the SORN VA 117VA10NA6/ 85 FR 7389 articulates the use of EPD information.

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

4. System Changes

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

No

K. Will 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. It must also match the information provided in question 3.4 of the PTA.

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

- ☒ Name
- ☒ Social Security Number
- ☐ Date of Birth
- ☐ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☒ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☒ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers[1]
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☐ Medical Records
- ☐ Race/Ethnicity
- ☒ Tax Identification Number
- ☐ Medical Record Number
- ☐ Gender
- ☐ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Data Elements (list below)

Other PII/PHI data elements: Deduction amount, Balance amount, Device ID, Employee Payroll Deduction Account Number

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

PII Mapping of Components (Servers/Database)

VCS-AIS consists of 4 key components (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by VCS-AIS and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
HRPAS	YES	YES	SSN	Required for Payroll Deduction performed by the US Treasury, for HR-PAS to check for Bankruptcy Flag, and Treasury Offset Program (TOPS) use to collect debits on delinquent EPD accounts.	Pay file is securely transferred to Treasury. Direct connect provides security hardened, point to-point file transfers to lessen dependency on unreliable File Transfer Protocol (FTP) transfers. It is optimized for high-volume delivery of files within and among enterprises
POMS Database/EPD	Yes	Yes	Full name, Mailing Address, Phone number, Email	Treasury Offset Program (TOPS) use to collect debits on delinquent EPD accounts.	Two-factor authentication (2FA), Limit access through Group policies

			address, financial account information, Social Security Number		hosted within AITC environment.
RAPP1	Yes	Yes	Full name, Mailing Address, Phone number, Email address, Social Security Number, Financial Account Information, Tax Identification Numbers	Expense report payments to employees and supplier payments to contract workers	Pay file is securely transferred to Treasury. Direct connect provides security hardened, point to-point file transfers to lessen dependency on unreliable File Transfer Protocol (FTP) transfers. It is optimized for high-volume delivery of files within and among enterprises
VCS-TOP MDP	Yes	Yes	Social Security Number, Full Name Mailing Address, Phone Number, Email Address	Required for collecting written off EPD Debt for referral to the VA Debt	VA Debt Management Center referral file is transferred to the mainframe using SFTP.

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?

Regarding EPD, individual information is collected directly from the individual as part of applying for an EPD card. Regarding Special Order, individual information is collected directly from the individual as part of placing an order. HR-PAS is also used to validate or update stale data used for debit collections.

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.

Information collected comes directly from an authorized VCS customer which could be a Veteran enrolled in VA Health Care, a family member of a Veteran enrolled in VA Health Care, VA Volunteer or VA employee. In this case HR-PAS crosschecks information to and from Treasury for EPD.

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

Retail Accounting Procurement Technology Organizational Reporting (RAPTOR) creates invoices and orders, aggregate inventory, pricing management, promotion management, Operation reports. etc.

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?

Regarding the EPD program, information is collected via a provisioning agreement form (no official number on the document). The customer completes a participating provisioning agreement form which must be approved by both the local Canteen Chief (or designee) and the local VA Payroll Office. The local canteen manager must obtain approval from the local VA payroll office and ensure the individual meets the criteria. Approval by the local VA Payroll Office means the VA employee: is a full or part-time VA employee who do not have a salary garnishment preventing payroll deduction payment and is not in the process of separation; is not under a federal tax levy; is not restricted by a court ordered bankruptcy and is not, to the knowledge of the Payroll Office, in the process of filing for bankruptcy. Temporary employees must be on a minimum Not to Exceed one year appointment and have been in a continuous pay status for at least six months. Approval by the local Canteen Chief means the VA employee: is not an intermittent and fee basis employee, has no outstanding amounts owed to VCS and is not known to have other employment problems leading to default or an inability to pay. Employees

in a without pay status and employees who have previous EPD write-offs will not be authorized to use EPD. Once this is approved and customer information is entered into the EPD system, the form must be destroyed. Information is manually typed into the EPD system for the customer card to be ordered, issued and used to make purchases. Regarding Special Order, while speaking with the customer on the phone, and includes the following information including Customer Name, "Ship To" Address, Telephone Number. Orders may also be placed via email in certain circumstances. However, there is no centralized database maintained of customer information by Special Order. Each purchase order is maintained separately with customer information. EPD is a benefit offered to VA employees, one of VCS' authorized customers, and accounts for about 40% of VCS sales. Due to its sales contribution, it allows VCS to sustain operations and contribute to VA quality of life programs. It is the individual's choice to decide whether they would like to enroll in the EPD program; however, the individual must be authorized and approved to use EPD. The information collected will be used by VCS and the local VA payroll office to determine if an individual is eligible to participate in the Electronic Payroll Deduction Program (EPD). To determine eligibility, the individual must first fill out a participation agreement (manual, handwritten form) and provide to the local canteen manager. Information provided on the agreement includes the name, social security number, VA station number, phone extension, email address. Accuracy of the information is dependent on what the individual writes on the agreement and what is manually entered into the EPD application by the local canteen manager. VCS can correct input errors in the EPD application. The information collection will also be used to establish an EPD account and administer EPD account transactions. It allows the individual to make purchases in VCS locations using their EPD account. Information collected may be disclosed to authorized VCS/VA employees responsible for administering and recording purchase and payment transactions to EPD accounts. For Special Order, the information collected is used to place a customer order.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, what is the form's OMB control number and the agency form number?

This system is not subject to the paperwork reduction act.

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.

The Local VA Payroll Office must approve the employee requesting EPD participation and that the individual meets the criteria (i.e., is an active-duty employee of the VA not in process of separation, is not under federal tax levy, is not restricted by court ordered bankruptcy and is not the process of filing for bankruptcy.) The local Canteen Chief must approve the individual to ensure they meet the criteria to include the individual has no other outstanding debts to the VCS.

It is also checked against HR-PAS databases. The system will undergo automated and manual test cases to ensure the validity of the data. For Special Order, the customer is asked a series of questions to determine if the customer is eligible to shop with VCS (i.e., Veteran enrolled in VA Healthcare, VA employee). Once it is determined the customer is eligible to shop, then the information provided is relied upon by the customer to make certain it is accurate. There are no databases or systems used by Special Order to make sure the customer information is accurate.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

For VCS-TOP manual review is performed for EPD debt to be collected. During the Monthly audit cycle VCS Debt Financial Management Center checks the VCS-TOP application data to update the current records. After VCS Financial personnel review the data, it is sent though STFP to the AITC Mainframe where the DMC personnel pull the data and review it for a second time. After the review is completed the VCS-TOP data is updated in accordance with VA policy.

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

VCS AIS operates under the authority of 38 U.S. Code Chapter 78 - VETERANS' CANTEEN SERVICE. For the collection of customers EPD information and permission to use the VCS Payroll Deduction System to make purchases, refer to System of Record 117VA10NA6/ 85 FR 7389.

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?

<u>Principle of Individual Participation:</u> 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: 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: To ensure business continuity and minimize potential damage due to unauthorized access, VCS maintains role-based access control to protect PII, other sensitive and proprietary information from intentional or accidental disclosure, modification, erasure, or copying, as well as VCS resources from misuse. This control provides VCS with the ability to restrict, monitor, and protect the confidentiality, integrity, and availability of VCS resources. VCS has implemented logical access control as one of the safeguards used to prevent unauthorized access to VCS's sensitive or critical information and to minimize the impact to, or from, security breaches. VCS access control measures, not only can it control who or what is to have access to VCS resources but also the type of access permitted.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
Name	Used to identify the Vendor/ Used to contact the individual	Used to identify the Vendor/ Used to contact the individual
Social Security Number	Required to make payments to an individual.	Required to make payments to an individual.
Home Mailing Address	Used to contact the individual	Used to contact the individual
Personal Phone Numbers	Used to contact the individual	Used to contact the individual
Personal Email Address	Used to contact the individual	Used to contact the individual
Financial Account Information	required for payment to a vendor	required for payment to a vendor
Tax Identification Number	required to make payments to a company	required to make payments to a company
Work Email Address	Email Address for workplace	Email Address for workplace
Work Address:	Address for workplace	Address for workplace

Work Phone & Extension	telephone and extension for workplace	telephone and extension for workplace
VA Station Number	work reporting station designated by VA	work reporting station designated by VA

EPD Customer information is collected and stored so VCS can provide payment deduction amounts from the employee's payroll account to HR-PAS and then on to the US Treasury. For the collection of customers EPD information and permission to use the VCS Payroll Deduction System to make purchases, refer to System of Record 117VA103 This is one of the benefits offered to VA employees by VCS. Approximately 40% of VCS business is attributed to EPD purchases. Social security number is needed to be able to refer the VA payroll system to have funds taken for the persons paycheck to apply to the balance of their EPD card. Social security number is needed for debt referral purposes if the person separates from the VA and does not pay off the remaining balance of their EPD card prior to separation. First name, last name, address, city, state, ZIP code, phone number as well as e-mail address need to be able to contact the person if there are issues encountered with their EPD account, and if the person separates from the VA and does not pay off the remaining balance of their EPD card prior to separation.

Special order customer information is required to place orders on behalf of customers who wish to purchase merchandise through VCS' 1-800 Special Order Call Center. The information is placed on a purchase order and transmitted to the appropriate vendor who will process, fulfill, and ship the order to the customer. This is one of the benefits offered to customers by VCS.

VCS may disclose information from this system of records to the U. S. Treasury Offset Program (TOPS) for the purpose of collecting unpaid balances from customers.

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?

System audit monitoring, analysis, and reporting are handled at the facility level at the AITC through the employment of Qradar Software. The primary pieces of information in the EPD database are: Customer Information Purchase and refund records at the transaction level Payroll payment data Customer acceptance of terms and conditions on the EPD participation agreement Card status (regular or gold member)To explain further, information collected about an individual is manually input by VCS (adding a new customer is completed at the local canteen level) into the EPD applications, and there are specific data fields that are manually filled out with the individuals' information (i.e., name, social security number, phone number, email

address) based on what the individual enters on the EPD participation agreement. The application is not flexible in that it does not have the ability to collect new information about a specific individual. The EPD application does offer some flexibility in that VCS Finance Center, or the local store manager can manually correct or update customer data, manually correct erroneously purchases or payments and manually add purchases, refunds, or payments. The only new information that is collected would be any new EPD transactions (i.e., purchases, refunds, or payments) based on the individual's usage of their EPD card. Purchases and refunds at the cash register are automatically updated to the customer account. As transactions are made, the customer's account balance is updated. Each pay period, the system computes the amount to be deducted from each customer's payroll. On payday, the system receives specific customer payment data and VCS receives a lump sum electronic payment. The system updates customer records with the payment data. Individuals have access to their EPD transactions and balances by accessing the EPD website on the VCS Intranet. Actions may be taken against individuals who stop making payments on their outstanding EPD balances. If an individual is delinquent on paying their EPD balance, the individual may be entered into the TOP application for VCS to be reimbursed for funds owed. The individual may have their wages or tax refunds garnished for the funds owed. There are various reports utilized by VCS Finance Center to ensure purchase and payment transactions are properly documented in the EPD system. Examples include Customers Without Payment Report and Customer Balances Report. The data in these reports are generated by what has been collected in the EPD system. The local store manager also has access to various EPD reports to include Canteen Customer Balances Report, Manual EPD transactions.

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.

N/A

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?

VCS is hosted on a secure VA network and is accessed through secure HTTPS transport protocol. All data and documents are stored in a secure VA data center. All data and documents are transferred via secure transmission protocols and only authorized persons can view the content of the documents. Firewall, VLAN and ACL are also implemented to limit network activity and availability to outside systems. At rest all servers are encrypted using FIPS 140-2 approved algorithms at the hardware or software level

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

In accordance with VA Handbook 6500, all users with access to VCS must complete basic security awareness training (including managers, senior executives, and contractors) of VA information systems or VA sensitive information as part of initial training and annually for recurring training. VCS also provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; when required by system changes; and annually thereafter. In addition, this VA implements DLP services and functions to limit available data to internal/external system.

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

SORN 117VA10NA6/ 85 FR 7389 clearly articulates the use of EPD information - Due to the age of software [Implemented in 2010], Oracle retail and finance are not integrated with PIV and is not supported. We use the account controls [service accounts] for process, which is audited weekly, monthly, quarterly, and yearly.

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?

VCS is hosted on a secure VA network and is accessed through secure HTTPS transport protocol. All data and documents are stored in a secure VA data center. All data and documents are transferred via secure transmission protocols and only authorized persons can view the content of the documents. The access to PII is determined by user job roles and functions. Example: Only Finances service employees and system administrators can directly access VCS AIS PII.

VCS System Access Requests: For users of the VCS system that require elevated privileges (system administrators, database administrators, etc.), Infrastructure Operations (IO) will manage user access using VA Form 9957 – Access Form. Regular user account management for end users of the VCS application (users at each VCS canteen location) will be handled by the VCS help desk staff. Security Services personnel will forward completed requests to the appropriate official for approval concurrence and then to the appropriate system administrator to

create the user account, issue a temporary first login password and notify the user. User access requests will be maintained and disposed of according to form management requirements. User access requests will be held for 3 years after the termination of each user account.

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

In accordance with VA Handbook 6500, all users with access to VCS must complete basic security awareness training (including managers, senior executives, and contractors) of VA information systems or VA sensitive information as part of initial training and annually for recurring training. Special Order employees must also follow Payment Card industry Data Security Standards (PCI DSS) requirements.

2.4c Does access require manager approval?

Yes

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

Yes

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

All personnel with access to VCS-AIS i.e. System administrator, DB administrator, Central office Finance, et are responsible for the safeguarding of PII information.

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*

Last name: Used for identification.
First name: Used for identification.
SSN: Used for identification.
Mailing Address - used for billing.
Zip code- Used for billing.
Telephone number: Used to contact.
Email address: Used to contact.
Financial Account Information: Used for billing.
Deduction amount: Used for billing.
Balance amount: Used for billing.
Device ID: transaction origin.

Employee Payroll Deduction Number: Used for billing.
Tax Identification Number: Used for billing.

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.*

Records for active participants in the Payroll Deduction Program are maintained indefinitely to include the EPD system. Records for participants who leave VA employment or voluntarily or involuntarily terminate their participation in the Payroll Deduction Program are retained for three years following the date the account attains a zero balance; or for three years following the date the account balance is written off following unsuccessful collection action.

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, VCS uses the Department of Veterans Affairs Records Control Schedule 10-1, 5550 – Canteen Services, which has been approved by NARA and is available on the internet by internet by clicking this link https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf.

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

According to the VHA Records Control Schedule, records are destroyed after 6 months and after audit by VCS auditors and the disposition authority - 349-S173. Please see the link below to the VHA Record Control Schedules (RCS):
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.

Under the jurisdiction of VHA, it is VA policy that all Federal records contained on paper, electronic, or other medium are properly managed from their creation through their final disposition, in accordance with Federal laws, the General Records Schedule (GRS) and VHA Records Control Schedule (RCS) 10-1. The GRS can be found at www.archives.gov. VA Directive 6300, Records and Information Management contains the policies and responsibilities for VA's Records and Information Management program. VA Handbook 6300.1, "Records Management Procedures", contains mandatory procedures for the proper management of eliminating data at the end of the retention period. Procedures are enforced by Records Management Staff and VA Records Officers. Per VCS Finance Center Canteen Operating Policies and Procedures (COPP), hard copies of the participation agreement must be destroyed on-site by shredding. According to VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization, Electronic data, and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed. When Version Date: October 1, 2022, Page 17 of 36 required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction.
file:///C:/Users/VACOOkereB/Documents/Directive_6500_24_Feb_2021%20(2).pdf"

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.

VCS AIS does not use any live or real data in the development or testing environments since our lower environments are clones of Production. After cloning, Social Security Numbers are scrambled before the new environment is opened to users. We use custom scripts to remove all Production SSN's. Passwords are locked and restricted Oracle Database by limiting user access through ePAS/SNOW Service Requests.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System 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: There is a risk that the information maintained by VCS 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, VCS adheres to the VA RCS schedules for each category of data it maintains. When the retention date is reached for a record, VCS administrators will carefully dispose of the data by the determined method as described in question 3.4. VA Handbook 6500.2, "Management of Data Breaches Involving Sensitive Personal Information (SPI)" contains the policies and responsibilities that VA components are required to follow to manage data breaches, including detection, correlation, notification, remediation, and reporting. A toll-free phone number will be established for data breach incidents potentially involving a large (500+) number of individuals. When one occurs, the number is activated and posted, along with a Health Information Technology for Economic and Clinical Health (HITECH) Press Release, on the VA Notices web page: http://www.va.gov/about_va/va_notices.asp.

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***
Personnel and Accounting Integrated Data (PAID) and Electronic Payroll Deduction (EPD)	Payroll deduction for item purchased	Social Security Number, Last Name, First Name, balance, and deduction amount	Encrypted batch file using FIPS 140 2 certified encryption module to protect the confidentiality of the data being transmitted.
EPD and VCS cash register system	Payroll deduction balances for customers to make purchases with accurate balances.	Customer name	Batch files between AITC, St. Louis Area and canteen register
Oracle RAP and VCS cash register sys	Transmit sales information to decrement stock on hand, report financial information and update cash registers with most current item information to be sold	Full Name, Financial Account Information	Batch file transmission
SPS Commerce/Direct	Procure retail and food merchandise	Full Name, Device IDs, Account information,	VCS Internet connection

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*
EDI, Oracle Retail Applications, POMS (EDI Preprocessor Tool	and products to sell in VCS operations and reimburse suppliers for ordered product.	Mailing Address, Phone number	Secured File Transmission Protocol
VCSTOP	Procure retail and food merchandise and products to sell in VCS operations and reimburse suppliers for ordered product.	Social Security Number, first name, last name, address, city, state, zip code, phone number, email address	Manual import of CSV file

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: The privacy risk associated with maintaining PII is that sharing data within the Department of Veterans Affairs could happen, and that data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

Mitigation: The principle of need-to-know is strictly adhered to by the Veterans Canteen Service personnel. Only personnel with a clear business purpose are allowed access to the system and the information contained within.

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***
GovX	VCS EPD transactions & balances.	Financial information, Full Name, Employee Payroll, Deduction Number,	MOU-ISA	SFTP - Secure Shell (SSH) Transfer of Files between GovX and VCS for EPD
SPS Commerce	EDI Information	Full Name, Financial Account Information	MOU-ISA	(SFTP) Secure Shell (SSH) Transfer SPS commerce

				and VCS-AIS for Invoice and orders.
U.S. Treasury	For EPD, Pay Files & Payee information	Pay files. Names, Addresses, Social Security Numbers, Financial Account Information	MOU-ISA	Direct circuit
DFAS	For VCS Employee Payroll Deduction	Social Security Number	MOU-ISA	Connect Direct

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

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

Follow the format below:

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

Mitigation: This risk is mitigated by the common practice of providing the Notice of Privacy Practices (NOPP) when eligible customers apply for benefits. Employees and contractors are required to review, sign, and abide by the National Rules of Behavior on a yearly basis as required by VA Handbook 6500 as well as complete annual mandatory Information Security and Privacy Awareness training. 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.

On the EPD participation agreement form which the individual fills out, the following Privacy Act Notice is included (attached as Appendix A): Privacy Act Notice: The following information is provided to comply with the Privacy Act of 1974 (PL 93-579). The information collected on this form will be used by VCS to identify you as an authorized VA employee customer eligible to participate in the Payroll Deduction Program (PDP); to establish a PDP account on your behalf; and to the administer PDP account transactions. Executive Order 9397 authorizes collection of your Social Security Number. Information collected may be disclosed to an authorized VCS/VA employee responsible for administering and recording purchase and payment transactions to your PDP account. It may also be disclosed to representatives of the U.S. Treasury Offset Payment System (TOPS); to authorized 3rd party debt collection agents; or to agents of any other authorized debt collection service for the purpose of collecting unpaid and /or past due balances for customers no longer employed by the VA. Disclosing of requested information is voluntary; however, failure to provide the information will prevent your participation in the PDP.
6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

Notice was provided
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.

Additional notice is provided by the system's System of Record Notice (SORN), Veteran Canteen Service (VCS) Payroll Deduction System, VA SORN 117VA10NA6, which can be viewed by clicking on this link: https://www.govinfo.gov/content/pkg/FR-2020-02-07/pdf/2020-02480.pdf A third form of notice is provided by this Privacy Impact Assessment, which is available online as required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii)

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.

Individuals have the opportunity or right to decline providing information as it is the individual's choice to enroll in the EPD program. However, if the individual does not provide all required information to use EPD, then a denial of service may occur. Specific information is required in order to set up the customer's EPD account and accurately process the EPD transaction through the EPD system and payroll. There is no penalty if the individual declines to provide all of the required information to establish an EPD account.

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.

Individuals seeking information regarding access to and contesting of records in this system may write, call, or visit the VCS Payroll Deduction Program Specialist at the Veterans Canteen Service Central Office (VCSCO–FC), St. Louis, Missouri 63125; telephone: (314) 845–1301.

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: There is a risk that an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by VCS prior to providing the required information.

Mitigation: The VA mitigates this risk by providing the individual with two forms of notice that the system exists, as discussed in detail in question 6.1, including the Privacy Impact Assessment and the System of Record Notice.

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 who wish to correct inaccurate or erroneous information should contact the VCS Payroll Deduction Program Specialist at the Veterans Canteen Service Central Office (VCSCO–FC), St. Louis, Missouri 63125; telephone: (314) 845–1301. Inquiries should include the person's full name, social security number, date(s) of contact, and return address.

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.

Individuals who wish to correct inaccurate or erroneous information should contact the VCS Payroll Deduction Program Specialist at the Veterans Canteen Service Central Office (VCSCO–FC), St. Louis, Missouri 63125; telephone: (314) 845–1301. Inquiries should include the person's full name, social security number, date(s) of contact, and return address.

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.

There is no automated process to contact individuals of missing or inaccurate information. It is the individual's responsibility to inform VCS of any account changes. If information was missing, the likelihood is the EPD application would not be processed, and the local canteen manager would contact the individual for the missing information to update the

system. Individuals who wish to determine whether this system of records contains records about them should contact the VCS Payroll Deduction Program Specialist at the Veterans Canteen Service Central Office (VCSCO–FC), St. Louis, Missouri 63125; telephone: (314) 845–1301. Inquiries should include the person's full name, social security number, date(s) of contact, and return address.

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 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 who wish to determine whether this system of records contains records about them should contact the VCS Payroll Deduction Program Specialist at the Veterans Canteen Service Central Office (VCSCO–FC), St. Louis, Missouri 63125; telephone: (314) 845–1301. Inquiries should include the person's full name, social security number, date(s) of contact, and return address.

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 the employee provides inaccurate or erroneous information when entering the information.

Mitigation: Any validation performed would merely be the employee personally reviewing the information before they submit it. Individuals are allowed to provide updated information for their records by updating the information and indicating that the new information supersedes the previous data.

Section 8. Technical Access and Security

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

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

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?

VCS System Access Requests: For users of the VCS system that require elevated privileges (system administrators, database administrators, etc.), Infrastructure Operations (IO) will manage user access using VA Form 9957 – Access Form.

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?

Other agencies do not have direct access to our systems. Information is shared via partner systems.

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.

Infrastructure Operations manages the VCS production platform with regard to security. Only IO system administrators and security personnel will be provided the highest-level access privileges on the systems (i.e., root accounts/passwords, system administrator accounts). Only user accounts with access privileges that cannot modify security configuration settings will be granted to other system users. Any requests for SUDO rights must be approved by IO. No executable scripts will be approved that have write ability. IO system administrators will load applications on the VCS platforms. Only the VCS team can change content and futures of the portal but are forbidden by Version Date: October 1, 2022, Page 28 of 36 policy to change or modify the operating system or any of its components. IO system administrators will be responsible for the anti-virus protection of the platform.

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.

Yes. The organization ensures that adequate documentation for all information systems and their constituent components are available, protected when required, and distributed to authorized personnel Users (government and contractor), will be granted a user ID and corresponding password for access to IO computing resources only upon receipt of a valid, properly completed VA Form 9957 or through ePAS. All onboarding new contractors and employees are required to sign and agree to the VA's ROB found in VA 6500 Handbook

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 VA Combined Rules of Behavior (ROB) prior to gaining access to any VA information system or sensitive information. The rules are included as part of the 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 security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. All VA employees must complete annual Privacy and Security training. Users agree to comply with all terms and conditions of the National Rules of Behavior, by signing a certificate of training at the end of the training session.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 05 June 2023
3. *The Authorization Status:* Authorization to Operate
4. *The Authorization Date:* 22 July 2021
5. *The Authorization Termination Date:* 21 July 2024
6. *The Risk Review Completion Date:* 02 July 2021
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* HIGH

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.***

N/A

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)*

N/A

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
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.

TERESA JONES-PIRTLE

Digitally signed by TERESA JONES-PIRTLE
Date: 2024.02.15 14:20:15 -06'00'

Privacy Officer, Teresa Jones-Pirtle

WESLEY BROWN

Digitally signed by WESLEY BROWN
Date: 2024.02.20 10:42:29 -06'00'

Information System Security Officer, Wesley Brown

LISA LEONELLI

Digitally signed by LISA LEONELLI
Date: 2024.02.20 12:29:02 -07'00'

Information System Owner, Lisa M. Leonelli

APPENDIX A-6.1

VA System of Records Notices (SORNs):
Federal Register :: Privacy Act of 1974; System of Records

Notice of Privacy Practice (NOPP):
VHA Notice of Privacy Practices
VHA Handbook 1605.04: Notice of Privacy Practices

HELPFUL LINKS:

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

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

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

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