Privacy Impact Assessment for the VA IT System called:

Veteran Canteen Service
Point-Of-Sales (POS) Assessing

Veteran Health Administration
Veterans Canteen Services (VCS)

Date PIA submitted for review:

08/10/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Jones-Pirtle, Teresa	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 Leonelli	Lisa.Leonelli@va.gov	801-588-5214

Abstract

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

The Point-of-Sale (POS) information system allows VCS to process and tender retail (i.e., sales) transactions on a computer-based hardware terminal by accepting cash, credit cards, and other unique tenders. The POS information system's sales data is exported to VCS's Enterprise Resource Planning (ERP) software application which allows for robust enterprise reporting and VCS to procure retail inventory from external vendors. Point of Sale (POS) system is a COTS product used primarily to support the tender trading mechanism that utilizes in all 219 nation-wide canteens stores to allow veterans, their families and guests, care givers, and Veterans Affairs employees the opportunity to purchase VCS retail goods and consumable meals during their visits.

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.*

Point of Sales, Veteran Canteen Service (VCS)

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

The Veterans Canteen Service's (VCS) point-of-sale system is a national information system currently managed by VCS POS Support Team, Office of Information & Technology (OI&T). As a retail centric organization, VCS manages approximately 210 business operations in VA Medical Centers to provide its authorized customers (Veterans, VA employees, caregivers, and family members) reasonably priced merchandise within retail and hospitality concepts. The POS system functions as a non-customer facing, point-of-service (payment) application. VCS employees process sales and/or retail transactions with POS commercial-off-the-shelf (COTS) software applications that reside on the cash register. The POS information system utilizes a deployment model that requires a corporate data center (CDC) to be managed in a server-side, centralized environment at the Austin Information and Technology Center Page 2 of 25(AITC). The cash register (or client-side devices) is interfaced with the CDC via a wide-area-network (WAN). Transaction data is uploaded to existing VCS Information System-Automated Information Systems-which is also presently hosted at AITC.

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

VA Owned and VA Operated IS

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.

2000+ total number of users. The individuals typically Veterans, VA employees, care givers & family members. The Point-of-Sale (POS) information system allows VCS to process and tender retail (i.e., sales) transactions on a computer-based hardware terminal by accepting cash, credit cards, and other. Transactions will not be possibly when the individuals are affected. No PII is shared or transmitted. Only Financial Account Information via secure TLS 1.2 connection

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

The Point-of-Sale (POS) information system allows the Veterans Canteen Service (VCS) stores across the country to process and tender retail (i.e., sales) transactions on a computer-based hardware terminal by accepting cash, credit cards, and other unique tenders.

The POS system consists of the following components:

- Tills – computer hardware where the POS applications are installed
- the credit card reader and signature pad
- register UPC scanners with wired docking stations
- Flooid Beanstore – the point-of-sale system
- the Vision Estate Manager Application – device management
- the application server, located at the Austin Information Technology Center (AITC)
- database and database server, located at the AITC.

The Tills have undergone technology refresh. All windows7 tills have now been successfully upgraded to Windows 10 Elo tills. The new computers use VA-supported monitoring tools such as BigFix and anti-virus software. The Tills are managed by Peraton and the VA Office of Information Technology (OIT). The credit card reader and signature pad are attached as peripherals to the Tills. The credit card readers have a network-based interface to a third-party payment authorization vendor. The Vision Estate Management Application (Estate Management) is used to monitor and manage the health and configuration of the tills.

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

VCS POS system share/receive and transmit financial data such as EPD#, Employee payroll Deduction (EPD#), Transaction ID, Transaction Date & Time & Full Name to other external IT systems such as SVS Tender and Retail Merchant Connect Multi via TLS encryption. The systems also have valid MOU ISA for the inter connection

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.

Only Financial Information and First Name is transmitted via secure TLS 1.2 connection

3. Legal Authority and SORN

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

The authority of maintenance of the system listed in question 1.1 falls under Title 28, United States Code, title 38, U.S.C., sections 501(a), 1705, 1710, 1722, and 5317." VCS's current System of Record is 117VA10NA6 (Veterans Canteen Service (VCS) Payroll Deduction Program (PDP), Point of Sale (POS) Help Desk and eCommerce-VA) https://www.oprm.va.gov/docs/Current_SORN_List_7_1_2022.pdf Authorization Decision: Authorization to Operate (ATO)
Authorization Date:17-Jul-2023
Authorization Termination Date: 14-Oct-2023
Type Authorization: No
Overall Risk Score: Very High
Highest System Data Classification: Unclassified

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?

A SORN 17VA10NA6 - Veterans Canteen Service (VCS) Payroll Deduction Program (PDP), Point of Sale (POS) Help Desk and eCommerce-VA is in place and will not require to be changed or modified with this update. The POS solution is currently an on-premises system and not cloud based. FedRAMP requirements do not apply to this solution. The system has been identified as a medium risk since PII and PHI information is not stored anywhere in the back-end infrastructure. Any leaks of information would have a very low impact to the VA whether it be intentionally or unintentionally.

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)
☒ Employee Pay Deduction (EPD)
☒ Transaction ID
☒ Transaction Date/Time
☒ Employee Gift Card Number

PII Mapping of Components (Servers/Database)

VCS POS Assessing consists of 3 key components (databases). Each component has been analyzed to determine if to determine if any elements of that component collect PII. The type of PII collected by VCS POS Assessing 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
EPD	**Yes**	**No**	Customer Name Financial Account Information Employee Payroll Deduction (EPD#), Transaction ID, Transaction Date/Time, Full Name	To process transactions completed with EPD	Secure File Transport Protocol
Oracle Financials	**Yes**	**No**	Customer Name Financial Account Information Employee Gift Card Number Transaction ID, Transaction Date/Time, Full Name	To process transactions completed with Gift Card	Secure File Transport Protocol
Retail Sales Audit (ReSA)	**Yes**	**No**	Store Inventory Item Counts Product details.	Process product details.	Secure File Transport Protocol

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?

EPD Tender:

EPD data elements listed at Section 1.1 will be sourced from three separate entities: 1) VCS's EPD Legacy Server hosted at AITC, 2, VCS's EPD Transaction Authorization Legacy Server hosted at STL Area 657 and 3) the VCS customer during a transaction's duration.

Credit Card Tender:
Credit Card data elements listed at Section 1.1 will be sourced from the VCS Customer's personal credit card.

Help Desk (Software Support) Contracted Service:
Help Desk data elements listed at Section 1.1 will be sourced directly from the VA employee during a Help Desk call or email with the COTS vendor's technical representative

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 is coming from external IT systems such as SVS Gift Card System and Tender Retail Merchant Multi (MCM) WorldPay. Financial Account Information is shared between POS and Gift Card System to complete purchases done using SVS gift card via PCI DSS industry security standard. Similarly financial account information is shared between POS and Tender Retail Merchant Connect Multi (MCM) WorldPay via TLS over https connection to complete purchases done using credit card.

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

VCS and contractor end-users will be able to generate reports from the application's existing data elements to develop an enterprise-wide data about the contracted service. The Vision Estate Management Application (Estate Management) is used to monitor and manage the health and configuration of the tills. The Estate Management provide reports on the current status of tills specific to canteen store that's used during troubleshooting or analysis

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?

EPD Tender:
EPD data elements are collected by the information system by the following methodologies:

EPD Card Swipe Transaction -> EPD cards are issued to VCS customers, and these physical tenders are required to process an EPD transaction at the POS terminal. If VCS customer elects to use
EPD Cards then transaction data will be captured by the point-of-sale software, and data elements such as EPD, Transaction ID will be used to either authorize or decline the transaction.

EPD Manual Entry Transaction -> An EPD manual entry transaction would be initiated by a VCS customer due to his/her unavailable Employee Payroll Deduction (EPD) card. Consequently, he/she would be required to know the entire account number, show PIV Badge issued by VA to verify EPD card holder identity, the customer would then manually key-in the data elements into the point-of-sale Pin Pad device for processing.

EPD Electronic Journal Query -> The VCS POS application will store the following transaction receipt information such as first name, last name, and transaction information on the servers

Credit Card Tender: A VCS customer who elects to use credit card inserted or
(PED) to complete the transaction. Debit Card purchases are automatically converted to a credit card (cc) transaction.

Help Desk (Software Support) Contracted Service:
The COTS vendor will collect Help Desk data elements by telephone or email. In the telephone methodology, the COTS vendor will collect the data elements verbally over the telephone and they will be transcribed into a contractor owned and operated software application. In the email methodology, the COTS vendor will receive the data elements in an email message and/or email attachment that has been sent to a contractor owned and operated domain. After the information has been successfully received by the vendor, the information will be transcribed into a contractor owned and operated software application

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 not collected on a form.

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.

EPD Tender:

VCS's EPD tender has systematic checks and balances that validate the data element's accuracy; this information is documented in VCS's current System of Record 117VA10NA6 (Veterans Canteen Service (VCS) Payroll Deduction Program (PDP), Point of Sale (POS) Help Desk and eCommerce-VA)

Credit Card Tender:
During the course of a transaction, credit card data elements are validated by the Department of Veterans Affairs Authorizing Agent WorldPay - and the customers card issuing bank.

Help Desk (Software Support) Contracted Service:
Help Desk information collected by the COTS vendor will have systematic checks and balances between the Help Desk technician and VCS staff that will allow either party to manually validate and revise the call ticket information throughout its lifecycle.

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.

The Point-of-Sale (POS) information system allows the Veterans Canteen Service (VCS) stores across the country to process and tender retail (i.e., sales) transactions on a computer-based hardware terminal by accepting cash, credit cards, and other unique tenders. All users use PIV cards to access tills. Every administrator has the same role and cannot grant or revoke other user access. For IBM Web Sphere, admin users access URL via the secured admi accounts on WebSphere Application Server (WAS) for role assignment.

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

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

The authority of maintenance of the system listed in question 1.1 falls under Title 28, United States Code, title 38, U.S.C., sections 501(a), 1705, 1710, 1722, and 5317." VCS's current System of Record is 117VA10NA6 (Veterans Canteen Service (VCS) Payroll Deduction Program (PDP), Point of Sale (POS) Help Desk and eCommerce-VA) https://www.oprm.va.gov/docs/Current_SORN_List_7_1_2022.pdf

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.

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

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

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

Privacy Risk:

1, If the POS information system's EPD, credit card, and Help Desk data elements are not utilized per the Veterans Canteen Service's operational practices and standards, then the agency's customer can lose confidence in the federal government's ability to secure and appropriately process personal information.
2, If the POS information systems client-side devices are maliciously accessed by unauthorized personnel, then EPD and credit cardholder data could potentially by stolen or modified on the cash register devices. 3, If VCS does not solicit PII directly from its customers for the EPD and Credit Card tenders, then the probability of fraudulent cardholder activity could increase.
4, If VCS does not have policies and procedures for DHS to ensure that PII data is protected, then the agency may unnecessarily increase the probability that data stewardship guidelines mandated by federal legislation or agency-specific policies on, and procedures will be violated.

Mitigation:

1, VCS will have its POS Information System annually assessed by the PCI council to ensure that security standards set forth in the requirements have been successfully met. VCS EPD System of Record 117VA10NA6 will be assessed by the Privacy Owner and System Owner on a biannual basis to ensure compliance with VA and other federal legislation has been successfully met.
2, EPD and credit cardholder data will not be stored on the client-side devices to the maximum extent reasonable as dictated by PCI and VA Handbook requirements.
3, VCS customers are required to present cashiers physical EPD and credit cards in order for a transaction to be completed. If either EPD or credit cards transactions exceed a total of $25.00, the VCS Cashier will also verify the customer's identification and require the customer to sign his/her receipt. The process collectively ensure that VCS solicits personal information directly from the customer
4, In sustainment, VCS ensures that the agency and/or contractor will adhere to federal law or governmental policy as deemed necessary by the Information System Security Officer (ISSO), Privacy Officer (PO), Contracting Officer Representative (COR), and Contracting Officer (CO).

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.

VA Employee Name – Used to identify the employee in the transaction
Personal Phone Number(S) - Used to contact the Individual
Personal Email Address - Used to identify or contact the employee.
Financial Account Information – Used to verify/approve transactions with data elements such as Card No, Transaction ID and Date/Time.

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.

EPD Tender: EPD data applications via a transaction log (TLog). For the EPD transaction set, the EPD Transaction Server hosted at STL Area 657 creates the following cursory details associated with the EPD account: a unique reference number, a unique authorization number, a truncated EPD account number, the authorization account balance, the customer's first name, and the customer's last name. The cursory details are stored in the EJ, and VCS end-users have the ability to retrieve a receipt associated with an EPD transaction based on any transaction set data elements (reference Section 1.3). VCS end-users will be able to create new data elements about EPD transaction set usage, but these new items will not be directly tied back to a customer account. Reports on EPD data elements do not exceed the present boundaries detailed in VA System of Record 117VA10NA6.

Credit Card Tender:
When a credit card successfully tendered, WorldPay will return a host of cursory details about the transaction to credit card payment application: a unique record number, the transaction's status, the credit card's input methodology, the credit card issuer, a transaction code, a partially truncated credit card account number (i.e last 4 digits) a completely truncated expiration date, the transactions total amount, the transactions total purchase amount, the transactions gratuity amount, the transactions cash amount, an authorization number, a unique reference number. The credit card payment application will export these cursory details to the point-of-sale software's credit card handling module, and a credit card transaction log will be created and stored within the POS information system.

Help Desk (Software Support) contracted Service: Help Desk data elements (section 1.2) will be stored on the COTS vendor's hosted Help Desk call ticket tracking application. VCS and contractor end-users will be able to generate reports from the application's existing data elements to develop an enterprise-wide data about the contracted service. No new or previously unutilized information about the VA employees will be incorporated into the records.

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.

If VCS customer elects to use
EPD Cards then transaction data will be captured by the point-of-sale software, and data elements such as EPD, Transaction ID will be used to either authorize or decline the transaction

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 communications between POS and external systems are secured via HTTPS and use TLS v1.2

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

No SSNs are retained on the POS system

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

POS do not share or receive PII/PHI data. However, the financial account information such as Card No, Transaction ID and Date/Time are safeguarded using https traffic

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:

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

<u>Principle of Use Limitation:</u> 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?

Employee Payroll Deduction (EPD):
VCS requires cashiers to complete mandatory cash and asset control training, as well as VA Information Security & Privacy training, prior to operation of a point-of-sale system. If a cashier does not remain current on his/her training status, management can temporarily or permanently prohibit him/her from processing POS transactions. Additionally, System of Record 117VA10NA6 details the system controls currently in place with EPD cardholder data elements, as it relates to the existing server-side infrastructure and client-side devices. Security controls are documented in the System of Record known as eMASS.

Credit Card Tender:
VCS requires cashiers to complete mandatory cash and asset control training, as well as VA Information Security & Privacy Awareness training, prior to operation of a point-of-sale system. If a cashier does not remain current on his/her training status, management can temporarily or permanently prohibit him/her from processing POS transactions.

Help Desk (Software Support) Contracted Service:

Help Desk data elements will be subject to VA contractor requirements that will ensure that the information system that's utilized and the personnel used adhere to security controls to include annual training, NIST security controls for the information system, and the contract's data ownership contract clauses

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

criteria, procedures, controls and responsibilities are documented in Access Control SOP

2.4c Does access require manager approval?

Yes, access require VCS Product Manager approval

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

NA as no PII is shared/transmitted or received

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

ISO, POS Product Manager

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*

EPD Tender: Within the POS information system only, the following EPD data elements are retained: VA Employee First Name, VA Employee Last Name, transaction history stemming from the use of the EPD card, a truncated EPD account number, customer account balance, a transaction reference number, and a transaction authorization number.   Credit Card Tender: Within the POS information system only, the following Credit Card Tender data elements will be retained: a unique record number, the transaction's status, the credit card's input methodology, the credit card issuer, a transaction code, a partially truncated credit card account number (i.e last 4 digits) a completely truncated expiration date, the transaction's total amount, the transaction's total purchase amount, the transaction's gratuity amount, the transaction's cash amount, an authorization number, a unique authorization number, and a unique reference number. Help Desk (Software Support) Contracted Service: Within the POS Information system only, the following data elements will be retained: VA employee first name, VA employee last name, VA employee work phone number, VA work address, and VA employee work email address, and all miscellaneous comments about a call ticket's service history.

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.*

EPD Tender: Since the POS information system will store EPD transaction data in the Electronic Journal, the agency requires the information to be retained for 1 year before archival occurs. Records for EPD tender participants will continue to comply with VA System of Record 117VA10NA6. The SORN states "Records for active participants in the Payroll Deduction Program are maintained indefinitely. Records for active participants in the Payroll Deduction Program are maintained indefinitely. Records for participants who leave VA employment voluntarily or involuntarily terminate their participation in the payroll deduction program are retained for three years following the data the account attains a zero balance; or for three years following the data the account balance is written off following unsuccessful collection action.” The EPD participants did not have their records migrated to the POS information system.

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

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA Records Officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner.
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, the retention schedule (DAA-0015-2018-0003) has been approved by the National Archives and Records Administration and has been published on the Federal Register on April 23, 2020, Vol 85, No 79, Pages 22798-22801. Records management is accomplished using Technical Reference Model (TRM) approved software that automatically gathers documents that are meeting disposition requirements EPD Tender: The VA Records Office and the National Archives and Records Maintenance Administration have approved a retention schedule for the POS information system's EPD tender data elements Record and Control Schedule 5550(25) Credit Card Tender: The VA Records Office and the National archives and Records Maintenance Administration have approved a retention schedule for the POS information system's Credit Card tender data elements; Record and Control Schedule 5550(36) Help Desk (Software Support) Contracted Service: The VA Records Office and the National Archives and Records Maintenance Administration have not approved a retention schedule for the POS Information system's Help Desk Service data elements

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

EPD Tender: Since the POS information system will store EPD transaction data in the Electronic Journal, the agency requires the information to be retained for 1 year before archival occurs. Records for EPD tender participants will continue to comply with VA System of Record 117VA10NA6. The SORN states “Records for active participants in the Payroll Deduction Program are maintained indefinitely. Records for active participants in the Payroll Deduction Program are maintained indefinitely. Records for participants who leave VA employment voluntarily or involuntarily terminate their participation in the payroll deduction program are retained for three years following the data the account attains a zero balance; or for three years following the data the account balance is written off following unsuccessful collection action.” The EPD participants did not have their records migrated to the POS information system.

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.

EPD Tender: EPD Tender records will be stored and archived by VCS hosting provider -AITC- at the AITC Corporate Data Center. If authorized personnel elect to extract EPD transaction data from the Electronic Journal on a physical media-such as paper-they will be required to shred the document on-site via the VCS location's associated shredding company policies and procedures; this process would occur after information provides no direct purpose to a VCS job duty or function. Credit Card Tender: Credit Card records retained by the Government will not have SPI. For non-sensitive data elements provider-AITC-at the AITC Corporate Data Center. If authorized personnel elect to extract Credit Card transaction data from the Electronic Journal on a physical media-such as paper-they will be required to shred the document on-site via the VCS location's associated shredding company policies and procedures; this process would occur after information provides no direct purpose to a VCS job duty or function. Help Desk (Software Support) Contracted Service: Since the contractor will be required to create, store, and dispose of Help Desk service retained information, the vendor will be required to comply with VA Handbook 6300.1 and VA Handbook 6500.1 (as described in VA Handbook 6500.6 Appendix C Clause 3(c).

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.

There is no PII information stored on this system. Credit Card and EPD numbers are masked in the system during transactions; however, customer name is displayed on the record. The system does not use PII for research, testing, or training.

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:

<u>Principle of Minimization:</u> Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

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

Follow the format below:

<u>Privacy Risk:</u>
If the project unnecessarily retains EPD and Credit Card tender's data elements longer than required for standard agency/organizational business processes, then the data can lose integrity by unauthorized access or ill-performed disposal practices by government/contractor personnel.

<u>Mitigation:</u> Throughout the program lifecycle, only system administrators or high privilege users will have access to the data hosted at the AITC Corporate Data Center. VCS personnel at the local level will not have the necessary permissions to manipulate or alter data element retention methodologies.

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***
Oracle Financials	To process transactions completed with Gift Card	Financial Account Information - Gift Card Number, Transaction ID, Transaction Date/Time, & Full Name	Secure File Transport Protocol
Employee Payroll Deduction (EPD)	To process transactions completed with EPD	Account Information Employee Payroll Deduction (EPD) Transaction ID, Transaction Date/Time, & Full Name	Secure File Transport Protocol
Retail Sales Audit (ReSA)	Process product details.	Store Inventory Item Counts Product details.	Secure File Transport Protocol

4.2 <u>PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure</u>

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:

<u>Privacy Risk:</u> POS system only share Name, Financial Account Information such as EPD#, Transaction Date/Time and Transaction ID to be received/shared between POS and Internal IT systems. POS system leverages safeguards such as SFTP for all data transmission. No sensitive information is shared during transactions. If the POS information systems client-side devices are maliciously accessed by unauthorized personnel, then EPD and credit cardholder data could be potentially stolen or modified on the cash register devices. If there is a breach, then transaction data can be exposed.

Mitigation: VCS POS only authorize network access to a select group of Internal connections. PIV card is required for access to the device which grant users access to the POS system. System also have FIPS 140-2 compliant modules. Only system administrators or high privilege users will have access to the data hosted at the AITC Corporate Data Center. VCS personnel at the local level will not have the necessary permissions to manipulate or alter data element retention methodologies. All transmitted data from VCS POS - Authorization Accreditation Boundary are safeguarded using https encrypted traffic.
~~NA~~

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***
Retail Merchant Connect Multi (MCM) Store Value Solutions (SVS) Gift Card System	To complete purchases done via SVS	Financial Account Information Gift Card Number, (Employee Payroll Deduction (EPD#), Transaction ID, Transaction Date/Time, & Full Name	Interconnection Security Agreement/Memorandum of Understanding	Support Payment Card Industry Security Standard (PCI DSS).
Tender Retail Merchant Connect Multi (MCM) WorldPay	To complete purchases done via WorldPay	Financial Account Information - Credit Card Number, (Employee Payroll Deduction (EPD#), Transaction ID, Transaction, Date/Time, & Full Name	Interconnection Security Agreement/Memorandum of Understanding	TLS over HTTPS connection

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

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

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

Follow the format below:

Privacy Risk: If VCS does not establish data usage agreements with external contractors, then VCS's data may be unlawfully shared with external parties not authorized within the POS Information System's contract.

Mitigation: VCS POS has approved MOU-ISA's

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.

Privacy Act Notice: The following information is provided to comply with the Privacy Act of 1974 (PL 93579). 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. VCS'S EPD data elements are currently covered by System of Record 117VA10NA6 (Veterans Canteen Service (VCS) Payroll Deduction Program (PDP), Point of Sale (POS) Help Desk and eCommerce-VA) 2020-02480.pdf (govinfo.gov) https://www.oprm.va.gov/docs/Current_SORN_List_7_1_2022.pdf,

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

VCS'S EPD data elements are currently covered by System of Record 117VA10NA6 (Veterans Canteen Service (VCS) Payroll Deduction Program (PDP), Point of Sale (POS) Help Desk and eCommerce-VA) https://www.oprm.va.gov/docs/Current_SORN_List_7_1_2022.pdf

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.

No. Data elements described at Section 1.2 are mandatory in order for VCS to process retail transactions and to support its POS information system. If the customer does not provide his/her information, then VCS will not be able to provide retail service to the individual with these two specific tender options. A VCS customer, however, maintains the right to utilize cash, check, VCS gift certificates, and hospital-specific tenders as alterative payment methodologies.

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.

EPD Tender
System of Record 117VA10NA6 details the customers abilities to consent to the use of their information

Credit Card Tender
As a retail-centric organization, VCS's authorized customers voluntarily shop at the business operations, and customers, thus, provide their initial consent for VCS to capture credit card data elements described at Section 1.2 Customers personal information is protected by the privacy policies associated with their card issuing banks and the Veterans Canteen Service's compliance with the Privacy Act

Help Desk (Software Support) Contracted Service
For the Help Desk data elements, VA employees and VA contractors are required to have personal information disseminated to the third-party contractor in order for the job duties to be successful accomplished.

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

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:

<u>Principle of Transparency:</u> Has sufficient notice been provided to the individual?

<u>Principle of Use Limitation:</u> 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:

<u>Privacy Risk:</u> If the customer data elements described at Section 1.2 are not used according to internal policies and procedures or third-party contract terms and conditions, then the agency may violate legislative standards that require customer notification about the use of his/her personal information.

<u>Mitigation:</u> Internal agency use of customer data elements will be documented with a Memorandum of Understanding (MOU) interconnection agreement. VCS's third-party contract will incorporate the required information custodial requirements set forth in VA Handbook 6500.6.

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.***

EPD Tender:

Individuals are notified of procedures correcting their information as described in SORN - 117VA10NA6 Veterans Canteen Service (VCS) Payroll Deduction Program (PDP), Point of Sale (POS) Help Desk and eCommerce-VA

Credit Card Tender:
If the customer requires access to its credit card transaction information, he/she has the following options: 1) contact card issuing bank directly or 2) call the VCS Finance Center (VCSFC). The VCSFC has the ability to work with WorldPay to evaluate credit card transactions for potential disputes, errors, etc.

For the call ticket log, neither VCS, nor the Department of Veterans Affairs, will have the ability to allow customers to gain access to their own credit card information because transaction log information described at Section 3.1 is not directly tied back to a customer.

Help Desk (Software Support) Contracted Service:
If the Help Desk service's data elements are subject to the Privacy Act, then customers/VA employees will be able to submit a FOIA request to VCS's PO.

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).

Not Applicable

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.

Not Appliable

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.

EPD Tender:
Individuals are notified of procedures correcting their information as described in SORN 117VA10NA6 - Veterans Canteen Service (VCS) Payroll Deduction Program (PDP), Point of Sale (POS) Help Desk and eCommerce-VA

Credit Card Tender:

If the customer requires access to its credit card transaction information, he/she has the following options: 1) contact card issuing bank directly or 2) call the VCS Finance Center (VCSFC). The VCSFC has the ability to work with WorldPay to evaluate credit card transactions for potential disputes, errors, etc.

For the call ticket log, neither VCS, nor the Department of Veterans Affairs, will have the ability to allow customers to gain access to their own credit card information because transaction log information described at Section 3.1 is not directly tied back to a customer.

Help Desk (Software Support) Contracted Service:

If the Help Desk Service's data elements are subject to the Privacy Act, the customers/VA employees will be able to submit a request to the VCS Help Desk Support Services to have information corrected. Since Help Desk data elements will be stored by a third-party contractor, the Chief of Business Strategy will work directly with the contractor to mitigate an alleged error in an individual's information.

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.

EPD Tender: Individuals are notified of procedures correcting their information as described in SORN 117VA10NA6 - Veterans Canteen Service (VCS) Payroll Deduction Program (PDP), Point of Sale (POS) Help Desk and eCommerce-VA Credit Card Tender: Neither VCS, nor the Department of Veterans Affairs, will have the ability to allow customers to gain access to their own credit card information because transaction log information described at Section 3.1 is not directly tied back to a customer. If the Help Desk service's data elements are subject to the Privacy Act, then customer/VA by VCS's Chief of Business Strategy (or a designee) via email, phone, or employees will be notified telephone that a correction has been made.

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. ***<u>Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.</u>***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Credit Card Tenders:
VCS customers have the ability to make contact with their respective banking institutions to access credit card transaction information.

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: If a customer is unable to find out whether a project maintains a record relating to him/her, then VCS can be subject to unnecessary litigation risk if the information is inappropriately used by internal or external stakeholders

Mitigation: . Individuals can contact the VCS Help Desk Support Services by phone or email to have any information corrected

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 Administrator - Reserved for AITC and select VCS Central Office personnel. High information system privileges because both server and client-side application access will be granted in order for technical troubleshooting to occur.
- Manager - Reserved for senior management at VCS Central Office and VCS Field Operations Moderate information system privileges because supervisors will be able to access multiple information system retail applications, alter some application, store-specific options/functions,

and process sensitive retail transactions (i.e., returns, post-voids, cash drawer access, etc.); however, they will not be able to access/manipulate post transaction data

- Supervisors - Reserved for supervisors at VCS Central Office and VCS Field Operations Moderate information system privileges because supervisors will be able to access multiple information system retail applications and alter some application, store-specific options/functions; however, they will not be able to access/manipulate post transaction data
- Cashier - Reserved for hourly employees within Field Operations.
    - Lowest information system privileges because cashiers will have no ability to access/manipulate post transaction data or change application options/functions.

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?

VCS Help desk & Sustainment contractors have elevated privilege access to the tills. Supervisor role can perform operations like voids for going over certain $ thresholds; close out tills, run reports, perform spot checks to verify the amount of cash is accurate and match the report. Supervisors and managers set criteria for what PII can be shared

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.

System Administrators – High privileges
Managers - Reserved for senior mgmt at VCS central office and VCS field operations. Can access system retail applications but will not be able to access/manipulate transaction data
Cashiers – Reserved for hourly employee with field operations – cashiers will not have ability to access/manipulate post transaction data or change application options/functions.

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.

VA contractors at AITC will have access to the POS Information System's Server-side software applications. AITC contractors are presently subject to clearance requirements implemented and monitored by VA Enterprise Operations. VA contractors from the COTS vendor will have access to both server-side and client-side software applications. Per a Position Designation System and Automation Toll (PDAT) assessment, the vendor's personnel will be required to complete a SF-85 background check, prior to accessing the VA network or it's applications.
All contractors must first be granted a VA clearance and VA network account before we can provide

access to the systems. All contractors are required to sign Non-Disclosure Agreements prior to access to the systems.

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 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 security awareness training which all personnel must complete via the VA's Talent Management System (TMS). The rules state the terms and conditions that apply to personnel who are provided access to, or use of, information, including VA sensitive information, or VA information systems, such as no expectation of privacy, and acceptance of monitoring of actions while accessing the system. After the user's initial acceptance of the Rules, the user must reaffirm their acceptance annually as part of the security awareness training. All individuals requesting access are required to complete all VA trainings (VA Privacy and Information Security Awareness and Rules of Behavior Training, Privacy and HIPAA Focused Training and Information Security for IT Specialists Training) and must be authorized by a VA Project Manager

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Please provide response here
2. *The System Security Plan Status Date:* Please provide response here
3. *The Authorization Status:* Full ATO
4. *The Authorization Date:* 17-Jul-2023
5. *The Authorization Termination Date:* 14-Oct-2023
6. *The Risk Review Completion Date:* 14-Oct-2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* MODERATE

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

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

NA

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)*

No Cloud Technology is used

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.*

Not Applicable

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

No Cloud Technology is used.

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.

No Cloud Technology is used

9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as “Bots” or Artificial Intelligence (AI).

NO RPA software is used

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

ID	Privacy Controls
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: 2023.09.07 16:15:28 -05'00'

Privacy Officer, Jones-Pirtle, Teresa

WESLEY BROWN

Digitally signed by WESLEY BROWN
Date: 2023.09.08 09:11:24 -05'00'

Information System Security Officer, Wesley Brown

LISA LEONELLI

Digitally signed by LISA LEONELLI
Date: 2023.09.08 08:48:17 -06'00'

Information System Owner, Lisa Leonelli

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).

2020-02480.pdf (govinfo.gov)

https://www.oprm.va.gov/docs/Current_SORN_List_7_1_2022.pdf

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