DEPARTMENT OF VETERANS AFFAIRS

PRIVACY ACT OF 1974; SYSTEM OF RECORDS

AGENCY: Department of Veterans Affairs (VA).

ACTION: Notice of a Modified System of Records.

SUMMARY: As required by the Privacy Act of 1974, notice is hereby given that the Department of Veterans Affairs (VA) is amending the system of records currently entitled, ‘‘Veterans Canteen Service (VCS) Payroll Deduction Program (PDP)-VA’’ (117VA103) as set forth in the Federal Register 75 FR 26851. VA is amending the system of records by revising the System Name; System Number; System Location; System Manager; Purpose of the System; Categories of Individuals Covered by the System; Categories of the Records in the System; Record Source Categories; Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of Such Uses; Policies and Practices for Storage of Records; Policies and Practices for Retrievability of Records; Policies and Practices For Retention and Disposal of Records; Physical, Procedural, and Administrative Safeguards; Record Access Procedure; and Notification Procedure. VA is republishing the system notice in its entirety.

DATES: Comments on this amended system of records must be received no later than **[Insert date 30 days after date of publication in the Federal Register]**. If no public comment is received during the period allowed for comment or unless otherwise published in the Federal Register by the VA, the new system will become effective **[Insert date 30 days after date of publication in the Federal Register]**.

ADDRESSES: Written comments may be submitted through www.Regulations.gov; by mail or hand-delivery to Director, Regulation Policy and Management (00REG), Department of Veterans Affairs, 810 Vermont Avenue, NW, Room 1064, Washington, DC 20420; or by fax to (202) 273-9026 (Note: not a toll-free number). Comments should indicate they are submitted in response to "Veterans Canteen Service (VCS) Payroll Deduction Program (PDP)-VA'' (117VA103). Copies of comments received will be available for public inspection in the Office of Regulation Policy and Management, Room 1063B, between the hours of 8:00 a.m. and 4:30 p.m., Monday through Friday (except holidays). Please call (202) 461-4902 for an appointment (Note: not a toll-free number). In addition, comments may be viewed online at www.Regulations.gov.

FOR FURTHER INFORMATION CONTACT: Veterans Health Administration (VHA) Privacy Act Officer, Department of Veterans Affairs, 810 Vermont Avenue, NW, Washington, DC 20420; telephone (704) 245-2492.

SUPPLEMENTARY INFORMATION: The System Name is being changed from "Veterans Canteen Service (VCS) Payroll Deduction Program (PDP)-VA'' to "Veterans Canteen Service (VCS) Payroll Deduction Program (PDP), Point of Sale (POS) Help Desk and eCommerce-VA."

The System Number will be changed from 117VA103 to 117VA10NA6 to reflect the current organizational alignment.

The System Location is being amended to replace Austin Automation Center (AAC) with Austin Information Technology Center (AITC). This section will add POS Help Desk and VCS eCommerce Site information, which is maintained on a contractor-

owned data center located in their Service Desk Online (SDO) system in Coventry, United Kingdom (UK) and Phoenix, Arizona, respectively.

The System Manager has been amended to add the POS Help Desk and eCommerce Site official responsible for policies and procedures: Office of the Business Operations and Support, Veterans Canteen Service (103), Department of Veterans Affairs, 810 Vermont Avenue, NW, Washington, DC 20420. Addresses for VA facilities are listed in VA Appendix 1.

Purpose of the System is being amended to add for the POS Help Desk and eCommerce Site. The VCS records allow authorized VCS contractors to collect relevant data to the end of providing operational support to maintain both cash register systems and the eCommerce Site. User data will be used for incident reporting and help desk activities, site personalization, Email communication, product recommendations, order management and payment processing. The VCS system of records allows authorized VCS employees and contractors to collect VCS canteen addresses, VCS canteen phone numbers, VCS system users first and last name and VCS employee's VA Email addresses through an incident management system for the purposes of in-taking, troubleshooting and triaging VCS call tickets. The operations and maintenance portions must be reported by the end user to a VCS contracted designated help desk who has been designated to resolve the issue. Records would be used to identify issues, conduct follow-up on unresolved issues, perform trend analyses on types of call ticket issues, generate reports and analytics on call ticket trends and notify VCS management of call ticket volume and trends. The additional functions serve to

provide a modern system as an eCommerce platform that is comparable to commercial eCommerce sites.

The Categories of Individuals Covered by the System is being amended to define the types of user data covered by the POS Help Desk and eCommerce Site.

The Categories of Records in the System is being amended to include the POS Help Desk and eCommerce Site records include the following identification information:

-User First and Last Name, Prefix, Suffix

-User Email address

-User Gender

-User Date of Birth

-User Address, City, State, and Postal Zip Code

-User Military Affiliation

-User Site Behavioral Patterns

-User Site Purchase History

-User Phone Number

-User PDP Account Number

-User PDP Account Balance

-User Date of Purchase

-User Purchase Amount

-User Identification Control Number (ICN)

-User Security ID

-User Assurance Level

-User Credential Service Identifier

-User Identifier

-User Hash

-User Authentication Time

-Credit Card Number

-Credit Card CVV

-Credit Card Date of Expiration

-PayPal credentials

-VCS Canteen location including Address, City, State and Postal Zip Code

-VCS Canteen Phone Number; and

-Description of System or Application Issue.

Record Source Categories is being amended to include the POS Help Desk and eCommerce Site information in this system of records is provided by authorized VCS employees who call, Email or submit a call ticket to the vendor in order to report a system, application or operational issue relative to a system application. The updates also provide the ability to offer a modern eCommerce platform that is comparable to commercial eCommerce sites, to include custom site personalization, product recommendations and order management.

The Routine Uses of Records Maintained in the System is amending the language in Routine Use #11, which states that disclosure of the records to the DoJ is a use of the information contained in the records that is compatible with the purpose for which VA collected the records. VA may disclose records in this system of records in legal proceedings before a court or administrative body after determining that the disclosure of the records to the court or administrative body is a use of the information contained in the records that is compatible with the purpose for which VA collected the records. This routine use will now state that release of the records to the DoJ is limited to circumstances where relevant and necessary to the litigation. VA may disclose

records in this system of records in legal proceedings before a court or administrative body after determining that release of the records to the court or administrative body is limited to circumstances where relevant and necessary to the litigation.

Routine Use #14 is clarifying the language to state, “VA may disclose any information or records to appropriate agencies, entities, and persons when (1) VA suspects or has confirmed that there has been a breach of the system of records; (2) VA has determined that as a result of the suspected or confirmed breach there is a risk to individuals, VA (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, or persons is reasonably necessary to assist in connection with VA efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.”

Routine use #15 is being added to state, “VA may disclose information from this system of records to another Federal agency or Federal entity, when VA determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.”

Routine use #16 is being added to state, “VA may disclose relevant information to VCS contracted vendors, in order to provide a single point of contact for all incidents relative to VCS’ POS software application.” VA needs this routine use for VCS

contracted vendors to use the information to intake, troubleshoot and triage call tickets as appropriate. In some cases, the incident may need to be escalated to a third party vendor or VA Office of Information Technology (OI&T) for further review and troubleshooting.

Routine use #17 is being added to state, “VA may disclose relevant information to third party vendors for issues outside the scope of VCS software application vendor. This includes, but is not limited to notification of canteen location, contact information, canteen manager first and last name, VA Email address, and description of the issue.” VA needs this routine use for vendors to triage and troubleshoot customer transactions.

Policies and Practices for Storage of Records is being amended to include the POS Help Desk records are maintained electronically within the managed service database.

Policies and Practices for Retrievability of Records is being amended to include the POS Help Desk and eCommerce Site records are retrieved by Incident Number.

Policies and Practices For Retention and Disposal of Records to replace “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 date the account attains a zero balance; or for three years following the date the account balance is written off following unsuccessful collection action” with Payroll System Reports which include error reports, ticklers, and system operation reports, destroy when related actions are completed or when no longer needed, not to

exceed 2 years. (N1-GRS-92-4 item 22a). Reports providing fiscal information on agency payroll destroy after GAO audit or when 3 years old, whichever is sooner. (N1-GRS-92-4 item 22c). Information Technology (IT) Customer Service File records related to providing help desk information to customers, including pamphlets, responses to Frequently Asked Questions, and other documents prepared in advance to assist customers, destroy/delete 1 year after record is superseded or obsolete. (N1-GRS-03-1 item 10a). Help desk logs and reports and other files related to customer query and problem response; query monitoring and clearance; and customer feedback records; and related trend analysis and reporting, destroy/delete when 1 year old or when no longer needed for review and analysis, whichever is later. (N1-GRS-03-1 item 10b)."

Physical, Procedural, and Administrative Safeguards is being amended to include:

POS Help Desk and eCommerce Site -

1. Access to VA work and file areas is restricted to VA personnel and authorized contractors with a legitimate need for the information in the performance of their official duties. Strict control measures are enforced to ensure that access by these individuals is appropriately limited. Contractor and VCS employees are required to complete and adhere to annual VA security and privacy awareness training and rules of behavior and are VA cleared. Access is controlled by individual unique passwords or codes, which must be changed periodically by the users.

2. Physical access to the contractor's data processing center is generally restricted to contractor employees, custodial personnel, Federal Protective Service, and other security personnel. Access to computer rooms is restricted to authorized operational

personnel through electronic locking devices. All other persons gaining access to computer rooms are escorted. The only personnel who are able to physically access SDO are the Contractor's IT Team and emergency responders.

3. All data transmissions are encrypted to prevent disclosure of protected Privacy Act information. Access to backup copies of data is restricted to authorized personnel in the same manner as the data processing center.

Record Access Procedure is being amended to include for the POS Help Desk, individuals seeking information regarding access to and contesting of records in this system may write, call, or visit the VCS' Chief, Business Operations and Support at the Veterans Canteen Service Central Office (VCSCO), St. Louis, Missouri 63125; telephone; (314) 845-1200.

Notification Procedure is being amended to include for the POS Help Desk and eCommerce Site, individuals who wish to determine whether the system contains records about them should contact the VCS Chief, Business Operations and Support at the Veterans Canteen Service Central Office (VCSCO), St. Louis, Missouri 63125; telephone; (314) 845-1200. Inquiries should contain the person's full name, date(s) of contact, and return address.

The Report of Intent to Amend a System of Records Notice and an advance copy of the system notice have been sent to the appropriate Congressional committees and to the Director of the Office of Management and Budget (OMB) as required by 5 U.S.C. § 552a(r) (Privacy Act) and guidelines issued by OMB (65 FR 77677), December 12, 2000.

Signing Authority: The Senior Agency Official for Privacy, or designee, approved this document and authorized the undersigned to sign and submit the document to the Office of the Federal Register for publication electronically as an official document of the Department of Veterans Affairs. F. John Buck, Director, Office of Privacy Information and Identity Protection, Office of Quality, Privacy and Risk, Office of Information and Technology, Department of Veterans Affairs, approved this document on June 5, 2018 for publication.

Dated: February 4, 2020.

Amy L. Rose,
Program Analyst,
VA Privacy Service,
Department of Veterans Affairs.

SYSTEM NAME: Veterans Canteen Service (VCS) Payroll Deduction Program (PDP), Point of Sale (POS) Help Desk and eCommerce-VA (117VA10NA6)

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Individual PDP purchase records are maintained in the VCS office at each Department of Veterans Affairs (VA) health care facility. Addresses for VA facilities are listed in VA Appendix 1. In addition, information from these records or copies of records is maintained in a centralized electronic database at the Austin Information Technology Center (AITC), 1615 East Woodward Street, Austin, TX 78772. For the POS Help Desk, information is maintained on a contractor owned-data center located in their Service-Desk Online (SDO) system in Coventry, United Kingdom (UK). For the eCommerce Site, data is maintained in a contracted data center located at the Phoenix, Arizona hosting site.

SYSTEM MANAGER(S): PDP official responsible for policies and procedures: Office of the Chief Financial Officer, Veterans Canteen Service (103), Department of Veterans Affairs, 810 Vermont Avenue, NW, Washington, DC 20420. Officials maintaining the system: Chief of the Canteen Service at the facility where the individuals were associated. Addresses for VA facilities are listed in VA Appendix 1.

For POS Help Desk and eCommerce Site, official responsible for policies and procedures: Office of the Business Operations and Support, Veterans Canteen Service (103), Department of Veterans Affairs, 810 Vermont Avenue, NW, Washington, DC 20420. Addresses for VA facilities are listed in VA Appendix 1.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code, Part V, Chapter 78.

PURPOSE(S) OF THE SYSTEM: PDP records and information will be used to track customer purchases, payments and balances due to VCS. Records and information may also be used for the purpose of debt collection. The records and information may be used for management and analysis reports of VCS programs.

For the POS Help Desk and eCommerce Site, the VCS System of Records allows authorized VCS contractors to collect data relevant to system processing to include addresses, phone numbers, user's first and last name, and Email addresses for the purposes of sustaining order fulfillment, payment processing, in-take, troubleshooting and triaging of VCS call tickets. Issues concerning the operation and maintenance of the must be reported by the end user to a VCS contracted designated help desk employee who has been designated to resolve the issue. Records are used to identify issues, conduct follow-up of unresolved issues, generate reports, perform trend analysis and notify VCS management of results from treading to include types of call tickets and call ticket volume. The VCS system of records allows authorized VCS employees and contractors to collect VCS canteen addresses, VCS canteen phone numbers, VCS system users first and last name and VCS employee's VA Email addresses through an incident management system for the purposes of in-taking, troubleshooting and triaging VCS call tickets. The records on the eCommerce Site will be further used to deliver a commercial grade eCommerce platform that will include the ability to provide site customizations and product recommendations based on user browsing patterns, and modern order fulfillment and payment processing methods.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: The individuals covered by the system encompass permanent VA employees, also known as

customers, who participate in the VCS Payroll Deduction System, which permits them to pay for purchases in VCS canteens through deduction from their pay. For the POS Help Desk, the individuals covered by the system encompass VCS employees. The VCS eCommerce site covers the VCS customer base which includes Veterans enrolled in VA's health care system, their families, caregivers, VA employees, volunteers, and visitors.

CATEGORIES OF RECORDS IN THE SYSTEM: These records include the following Information for PDP:

-Customer identification information such as last name, first name, middle initial, social security number;

-Customer purchases made under the program;

-Timestamps for payments;

-Payroll payments, cash payments, refunds for returned merchandise, and refunds for overpayments;

-Customer account balances and amounts written-off as uncollectible;

-Customer pay status when customer is in a ''without pay'' status;

-Identification of VCS employees creating customer transactions is by manual or electronic data capture. Manual transactions can be traced by a user ID within the payroll deduction system that identifies the individual entering the manual transaction. Electronic transactions can be traced by cashier code of the cashier ringing the transaction into the cash register; and

-Customer station number and canteen of purchase.

The POS Help Desk and eCommerce Site records include the following identification information:

-User First and Last Name, Prefix, Suffix

-User Email address

-User Gender

-User Date of Birth

-User Address, City, State, and Postal Zip Code

-User Military Affiliation

-User Site Behavioral Patterns

-User Site Purchase History

-User Phone Number

-User PDP Account Number

-User PDP Account Balance

-User Date of Purchase

-User Purchase Amount

-User ICN

-User Security ID

-User Assurance Level

-User Credential Service Identifier

-User Identifier

-User Hash

-User Authentication Time

-Credit Card Number

-Credit Card CVV

-Credit Card Date of Expiration

-PayPal credentials

-VCS canteen location including Address, City, State and Postal Zip Code

-VCS canteen Phone Number; and

-Description of System or Application Issue.

RECORD SOURCE CATEGORIES: Information in this system of records is provided by the customers who participate in the PDP program, users of the VCS eCommerce Site, VA employees and various VA systems.

The POS Help Desk information in this system of records is provided by authorized users who call, Email or submit a call ticket to a VCS contracted vendor in order to report a system, application or operational issue relative to the system.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES: To the extent that records contained in the system include information protected by 45 CFR Parts 160 and 164, *i.e.*, individually identifiable health information, and 38 U.S.C. 7332, *i.e.*, medical treatment information related to drug abuse, alcoholism or alcohol abuse, sickle cell anemia or infection with the human immunodeficiency virus, that information cannot be disclosed under a routine use unless there is also specific statutory authority in 38 U.S.C. 7332 and regulatory authority in 45 CFR Parts 160 and 164 permitting disclosure.

1. VA may disclose information from this system of records to a private debt collection agent for the purpose of collecting unpaid balances from customers who have left VA employment without making full payment for purchases made under the program.

2. VA 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 who have left VA employment without making full payment for purchases made under the

program. VA needs to be able to collect unpaid balances from customers who have left VA employment without making full payment to VCS for purchases made under the program.

3. Disclosure may be made to the Federal Labor Relations Authority (FLRA), including its General Counsel, when requested in connection with investigation and resolution of allegations of unfair labor practices, in connection with the resolution of exceptions to arbitrator awards when a question of material fact is raised, and in connection with matters before the Federal Service Impasses Panel. The release of information to FLRA from this Privacy Act system of records is necessary to comply with the statutory mandate under which FLRA operates.

4. Disclosure may be made to officials of labor organizations recognized under 5 U.S.C. chapter 71 when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting working conditions.

5. Disclosure may be made to officials of the Merit Systems Protection Board, including the Office of the Special Counsel, when requested in connection with appeals, special studies of the civil service and other merit systems, review of rules and regulations, investigation of alleged or possible prohibited personnel practices, and such other functions promulgated in 5 U.S.C. 1205 and 1206, or as may be authorized by law.

6. Disclosure may be made to the Equal Employment Opportunity Commission when requested in connection with investigations of alleged or possible discrimination practices, examination of Federal affirmative employment programs, compliance with the Uniform Guidelines of Employee Selection Procedures, or other functions vested in the Commission by the President's Reorganization Plan No. 1 of 1978.

7. A record from a system of records maintained by this component may be disclosed as a routine use to the National Archives and Records Administration (NARA) for the purpose of records management inspections conducted under authority of Title 44 United States Code. NARA is responsible for archiving old records no longer actively used but which may be appropriate for preservation; they are responsible in general for the physical maintenance of the Federal government's records. VA must be able to turn records over to these agencies in order to determine the proper disposition of such records.

8. Disclosure of relevant information may be made to individuals, organizations, private or public agencies, etc., with whom VA has a contract or agreement to perform such services as VA may deem practicable for the purposes of laws administered by VA, in order for the contractor or subcontractor to perform the services of the contract or agreement. VA occasionally contracts out certain functions when this would contribute to effective and efficient operations. VA must be able to give a contractor whatever information is necessary for the contractor to fulfill its duties. In these situations, safeguards are provided in the contract prohibiting the contractor from using or disclosing the information for any purpose other than that described in the contract.

9. Disclosure from a system of records maintained by this component may be made to a Congressional office from the record of an individual in response to an inquiry from the Congressional office made at the request of that individual. Individuals sometimes request the help of a member of Congress in resolving some issues relating to a matter before VA. The member of Congress then writes VA, and VA must be able to give sufficient information to be responsive to the inquiry.

10. Disclosure may be made to a Federal, State or local agency, upon its official request, to the extent that it is relevant and necessary to that agency's decision regarding: the hiring, retention or transfer of an employee, the issuance of a security clearance, the letting of a contract, or the issuance or continuance of a license, grant or other benefit given by that agency. However, in accordance with an agreement with the U.S. Postal Service, disclosures to the U.S. Postal Service for decisions concerning the employment of veterans will only be made with the Veteran's prior written consent. VA must be able to provide information to agencies conducting background checks on applicants for employment or licensure.

11. VA may disclose information in this system of records to the Department of Justice (DoJ), either on VA's initiative or in response to DoJ's request for the information, after either VA or DoJ determines that such information is relevant to DoJ's representation of the United States or any of its components in legal proceedings before a court or adjudicative body, provided that, in each case, the agency also determines prior to disclosure that release of the records to the DoJ is limited to circumstances where relevant and necessary to the litigation. VA may disclose records in this system of records in legal proceedings before a court or administrative body after determining that release of the records to the court or administrative body is limited to circumstances where relevant and necessary to the litigation.

12. VA may disclose any information in this system, except the names and home addresses of Veterans and their dependents, which is relevant to a suspected or reasonably imminent violation of law, whether civil, criminal or regulatory in nature and whether arising by general or program statute or by regulation, rule or

order issued pursuant thereto, to a Federal, State, local, tribal, or foreign agency charged with the responsibility of investigating or prosecuting such violation, or charged with enforcing or implementing the statute, regulation, rule or order. VA may also disclose the names and addresses of Veterans and their dependents to a Federal agency charged with the responsibility of investigating or prosecuting civil, criminal or regulatory violations of law, or charged with enforcing or implementing the statute, regulation, rule or order issued pursuant thereto.

13. Disclosure to other Federal agencies may be made to assist such agencies in preventing and detecting possible fraud or abuse by individuals in their operations and programs.

14. VA may disclose any information or records to appropriate agencies, entities, and persons when (1) VA suspects or has confirmed that there has been a breach of the system of records; (2) VA has determined that as a result of the suspected or confirmed breach there is a risk to individuals, VA (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, or persons is reasonably necessary to assist in connection with VA efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

15. VA may disclose information from this system to another Federal agency or Federal entity, when VA determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs,

and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

16. VA may disclose relevant information to VCS contracted POS and eCommerce vendor, in order to provide a single point of contact for all incidents relative to the VCS system. This routine use permits VCS contracted vendors to use the information to process orders and payment, call intake, troubleshoot and triage call tickets as appropriate. In some cases, the incident may need to be escalated to a third-party vendor or VA Office of Information Technology (OI&T) for further review and resolution.

17. VA may disclose relevant information to third party vendors to analyze product recommendations, perform site customizations, process payments, and resolve issues outside the scope of the VCS system vendors. This information may include canteen location, contact information, canteen manager first and last name, VA Email address, issues description, site browsing patterns, purchase history, military affiliation, gender, and date of birth. This routine use permits third party vendors to triage and troubleshoot customer issues when the VCS vendor is unable due to the scope of their contract.

DISCLOSURE TO CONSUMER REPORTING AGENCIES: Pursuant to 5 U.S.C. 552a(b)(12), VA may disclose records from this system to consumer reporting agencies as defined in the Fair Credit Reporting Act (15 U.S.C. 168la(f)) or the Federal Claims Collection Act of 1966 (31 US.C. 3701(a)(3)).

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: PDP records are maintained primarily on a computer disk in a centralized database system. Paper records of program Participation Agreements and individual customer records are

maintained in canteen office files. The POS Help Desk and eCommerce records are maintained electronically within the respective vendors managed service databases.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: PDP records are retrieved by name and/or Social Security number of the participating VA employees or customers. The POS Help Desk records are retrieved by Incident Number. There is typically a three-letter mnemonic that identifies the customer with an incremented number following the mnemonic. eCommerce Site records can be retrieved by Email address or User Identifier data element.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Payroll System Reports which include error reports, ticklers, and system operation reports, destroy when related actions are completed or when no longer needed, not to exceed 2 years. (N1-GRS-92-4 item 22a). Reports providing fiscal information on agency payroll destroy after GAO audit or when 3 years old, whichever is sooner. (N1-GRS-92-4 item 22c). Information Technology Customer Service File records related to providing help desk information to customers, including pamphlets, responses to Frequently Asked Questions, and other documents prepared in advance to assist customers, destroy/delete 1 year after record is superseded or obsolete. (N1-GRS-03-1 item 10a). Help desk logs and reports and other files related to customer query and problem response; query monitoring and clearance; and customer feedback records; and related trend analysis and reporting, destroy/delete when 1 year old or when no longer needed for review and analysis, whichever is later. (N1-GRS-03-1 item 10b).

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

PDP-

1. Access to VA work and file areas is restricted to VA personnel with a legitimate need for the information in the performance of their official duties. Strict control measures are enforced to ensure that access by these individuals is appropriately limited. Information stored electronically may be accessed by authorized VCS employees at remote locations, including VA health care facilities. Access is controlled by individually unique passwords or codes, which must be changed periodically by the users.

2. Physical access to the Austin VA Data Processing Center is generally restricted to Center employees, custodial personnel, Federal Protective Service, and other security personnel. VA file areas are generally locked after normal duty hours, and the facilities are protected from outside access by the Federal Protective Service or other security personnel. Access to computer rooms is restricted to authorized operational personnel through electronic locking devices. All other persons gaining access to computer rooms are escorted.

3. All data transmissions are encrypted to prevent disclosure of protected Privacy Act information. Access to backup copies of data is restricted to authorized personnel in the same manner as the Austin VA Data Processing Center.

POS Help Desk and eCommerce Site-

1. Access to VA work and file areas is restricted to VA personnel and authorized contractors with a legitimate need for the information in the performance of their official duties. Strict control measures are enforced to ensure that access by these individuals is appropriately limited. Contractors and VCS employees are required to annually complete and adhere to VA security and privacy awareness training and sign the rules

of behavior. Access is controlled by individual unique passwords or codes, which must be changed periodically by the users.

2. Physical access to the contractor's data processing center is generally restricted to contractor employees, custodial personnel, Federal Protective Service, and other security personnel. Access to computer rooms is restricted to authorized personnel through electronic locking devices. All other persons gaining access to computer rooms are escorted. The only personnel who are provided physical access are the Contractor's Information Technology (IT) Team and emergency responders.

3. All data transmissions are encrypted to prevent disclosure of protected information. Access to backup copies of data is restricted to authorized personnel in the same manner as the AITC.

RECORD ACCESS PROCEDURE: Individuals seeking information regarding PDP 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.

For the POS Help Desk or VCS eCommerce Site, individuals seeking information regarding access to and contesting of records in this system may write, call, or visit the VCS' Chief, Business Operations and Support at the Veterans Canteen Service Central Office (VCSCO), St. Louis, Missouri 63125; telephone; (314) 845-1200.

CONTESTING RECORD PROCEDURES: (See Record Access Procedures above.)

NOTIFICATION PROCEDURE: Individuals who wish to determine whether this system of records contains PDP 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.

For the POS Help Desk and VCS eCommerce Site, individuals who wish to determine whether the system contains records about them should contact the VCS Chief, Business Operations and Support at the Veterans Canteen Service Central Office (VCSCO), St. Louis, Missouri 63125; telephone; (314) 845-1200. Inquiries should contain the person's full name, date(s) of contact, and return address.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: Last full publication provided in 75 FR 26851 dated May 12, 2010.

[FR Doc. 2020-02480 Filed: 2/6/2020 8:45 am; Publication Date: 2/7/2020]