
Privacy Impact Assessment for the VA IT System called:

# Centralized Administrative Accounting Transaction System (CAATS)

# Infrastructure Operations Authorization Support (IO-AS)
# Austin Information Technology Center (AITC)

Date PIA submitted for review:

03/11/2022

System Contacts:

*System Contacts*

| | Name | E-mail | Phone Number |
|---|---|---|---|
| Privacy Officer | Tonya Facemire | Tonya.Facemire@va.gov | (202) 632-7861 |
| Information System Security Officer (ISSO) | Jason Beard | Jason.Beard@va.gov | (512) 326-6380 |
| Information System Owner | James Ervin | James.Ervin@va.gov | (727) 201-7082 |

## Abstract

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

Centralized Administrative Accounting Transaction System (CAATS) is a web-based automated system that allows for the electronic input and approval of accounting source document/transactions, improvement of internal controls standardization of accounting entries, electronic audit trail, and separation of duties. CAATS is owned by the Office of Information Technology and sponsored by the Office of Financial Management (OFM). It is the central interface to Financial Management System (FMS) for both Veterans Benefits Administration (VBA) and National Cemetery Administration (NCA).

## 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:*

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *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.*
- *A citation of the legal authority to operate the IT system.*

- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *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?*

In 2003, CAATS was conceived by the US Department of Veterans Affairs (VA), Veterans Benefits Administration (VBA), Administrative and Loan Accounting Center (ALAC) in Austin, Texas. The initial development of the application was to support the VBA Chief Financial Officer's (CFO) centralization mandate when ALAC absorbed the administrative accounting functions performed at the Regional Offices (ROs) throughout the US. The initiative assumes that VBA will better serve Veterans through improved efficiency of resources. National Cemetery Administration (NCA) partnered with VBA on CAATS development to help design current and future functionality, to provide ongoing benefits to their field offices, and to support the mission they server more efficiently. CAATS is designed in a module/sub-module system.

There are 23 modules in CAATS:

- Obligations
- Budget
- Payments
- Accounts Receivable
- Deposits
- Benefit Debt
- Cost/Revenue-Suspense Transfers
- Accrual
- Purchase Card
- Manila (Manila Regional Office)
- VR&E (Vocational Rehabilitation and Employment) Service Group
- AAD (Administrative Accounting Division) Workload
- Workload Measurement
- LGY (Loan Guaranty)
- Paralympics
- Contract Exam
- Requisition
- Reconciliation
- System Administration
- Import/Export
- Reports and Document
- Workload Management
- Reports

Stations have the capability to submit various transactions, which are either approved or returned by designated staff. The approved transactions then interface with FMS.

CAATS currently has approximately 15,000 NCA and VBA users that depend upon the application to submit various financial transactions to FMS. 11,500 of the 15,000 users are Contract Exam users. On 10/1/2018, Compensation and Pension (Comp and Pen) decided to no longer utilize CAATS.
CAATS made significant contributions towards improving Veterans' lives and supporting VA's mission. The application provides comprehensive financial support services to VA and also directly impacts Veterans' daily lives in the following ways:

- The application supports our Paralympic Veterans by directly paying them (monthly) to practice and compete. In FY 2021, 197 Paralympic Veterans received service that resulted in 2,100 invoice payments being processed in CAATS totaling $1.8M.
- The application submits 27,000+ suspense payments to FMS allowing the payment of $254M+ to Veterans and the financial requirements for Veterans.

- Starting in December 2020 CAATS support the Office of Transition and Economic Development (OTED). OTED supports over 2,400 Veterans and made over 4,000 payments totaling more than $1.7M.
- The application is used to procure educational and vocational services for service-connected Veterans assisting them in maintaining employment, providing counseling, and providing specialized needs to Veterans. In FY21 a total of more than 15,000 invoices totaling more than $6M were electronically procured and invoiced through CAATS utilizing the Vocational Rehabilitation & Employment (VR&E) VetSuccess (National Workload) module. The payments were for services rendered to over 9,900 service-connected Veterans.
- The application submits payment transactions to FMS to send child support payments to the court for approximately 3,000 Veterans' Dependents.
- Lastly the application, supports the burial of 125,000 Veterans a year by streamlining NCA's purchase of grave liners.

CAATS uses the SORN 27VA047 and operates under the authority of Title 38, United States Code, Section 501. Routine Uses of Records Maintained in the System, Including Categories of Users and the Purpose of Such Uses pursuant to a legal process as defined in 5 U.S.C. 5520a.
The application is hosted at AITC and used throughout VBA, ALAC and NCA.

## 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 Account Information

☐ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers
☐ Vehicle License Plate Number
☒ Internet Protocol (IP) Address Numbers
☐ Current Medications
☐ Previous Medical Records
☐ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☐ Gender

☐ Integration Control Number (ICN)
☐ Military History/Service Connection
☐ Next of Kin
☐ Other Unique Identifying Information (list below)

Orders: Purchase Card Orders.
Charges and Reconciles: Used to verify authorized purchases.
Transfers: Accounting information.
Check Lists: Simple list of items purchased.
Reconcile Approvals: Approval of authorized purchase.
Card Management: Used to track the physical credit card.
Accrual Creation: Used for audit trails.

**PII Mapping of Components**

**CAATS** consists of **two** key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **CAATS** and the reasons for the collection of the PII are in the table below.

**PII Mapped to Components**

*PII Mapped to Components*

| 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 |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| CAATS Server 1 | Yes | Yes | Vendor Tax ID; Address | Validate as valid when issuing payment or other transactions | Secure File Transfer Protocol (SFTP) |
| CAATS Server 2 | Yes | Yes | Veteran's SSN and claim number | Used to create referral order | SSN & claim number encrypted in database |
| | | | | | |
| | | | | | |
| | | | | | |

**1.2 What are the sources of the information in the system?**

*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?*

*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 1.3 indicate why the system is using this source of data.*

*If the system creates information (for example, a score, analysis, or report), list the system as a source of information.*
*This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.*

CAATS receives data from field sites directly from a web interface. Additional data is received from Electronic Contract Management System (eCMS) and Credit Card System (CCS) via SFTP. CAATS provides centralization for administrative accounting functions. Stations have the capability to submit various transactions, which are approved or returned by designated staff. A nightly batch process runs to feed FMS with any approved transactions. The CAATS system automates the data transfer between VBA field stations and FMS. CAATS generates and sends transactions to FMS daily. It stores transactions and sends them all in one batch file daily. CAATS is accessed from VBA field stations (regional offices); NCA field stations (Memorial Service Network Offices – MSN's and Cemetery Finance Offices) as well as the VBA Administrative and Loan Accounting Center (ALAC) in Austin, Texas and the NCA Finance Division in Quantico, Virginia.

**1.3 How is the information collected?**

*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 technology used in the storage or transmission of information in identifiable form?*

*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.*
*This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.*

CAATS receives data from field sites directly from a web interface. Additional data is received from eCMS and CCS via SFTP.

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

*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.*

*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.*
*This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.*

The Centralized Administrative Accounting Transaction System (CAATS) performs financial management. CAATS uses financial information to measure, operate and predict the effectiveness and efficiency of an entity's activities in relation to its objectives.
CAATS manages accounting data such as assets, liabilities, fund balances, revenues and expenses associated with the maintenance of federal funds and expenditure of federal appropriations (Salaries and Expenses, Operation and Maintenance, Procurement, Working Capital, Trust Funds, etc.), in accordance with applicable federal standards (FASAB, Treasury, OMB, GAO, etc.). The systems management of obligations includes monitoring and reconciling unliquidated obligations to ensure that all unliquidated obligations are valid or cancelled.
Furthermore, CAATS management of accruals includes ensuring that all end of month, quarter and annual accruals are properly recorded and documented to ensure that all expenditures and expenses are properly recognized for reporting purposes. The system also provides management of payments including disbursements of federal funds, via a variety of mechanisms, to federal and private individuals, federal agencies, state, local and international governments, and the private sector, to effect payment for goods and services, or distribute entitlements, benefits, payroll, grants, subsidies, loans, or claims including the prevention of improper payments. Improper payments are any payment that should not have been made, or was made in an incorrect amount under statutory, contractual, administrative, or other legally applicable requirements. Improper payments are also those payments where an agency is unable to discern whether a payment was proper as a result of insufficient or lack of documentation. CAATS also manages other payables including disbursements of federal funds unrelated to payroll, credit cards or grants, via electronic payment or check.

**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*

CAATS uses the SORN 27VA047 and operates under the authority of Title 38, United States Code, Section 501. Routine Uses of Records Maintained in the System, Including Categories of Users and the Purpose of Such Uses pursuant to a legal process as defined in 5 U.S.C. 5520a.

The CAATS system exchanges data with the FMS (Financial Management System) via Secure File Transfer Protocol (SFTP) file exchanges. CAATS will download data from the FMS daily (including budgetary allowances, open advances, unapplied deposits, open receivables, and open obligation data) to keep a running total of these balances throughout the day. Also, a nightly batch process will then run to feed FMS with any approved CAATS transactions. CAATS then receives back the file from FMS the following morning indicating the transactions have accepted or rejected.
The CAATS system exchanges messages with eCMS (Electronic Contract Management System) via web services. CAATS interfaces multiple times each day sending requisitions to eCMS for processing and receiving Purchase Orders processed by eCMS back for obligation in FMS through CAATS. Status updates are also passed back and forth between eCMS and CAATS. The CAATS system receives purchase card transaction information via file exchanges with the VA CCS (Credit Card System). All system users are internal to the VA.

**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.*

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

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

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

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

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

Follow the format below when entering your risk assessment:
**Privacy Risk:** CAATS collects Personally Identifiable Information (PII) and other highly delicate Personal Health Information (PHI). If this information was breached or accidentally released to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to the individuals whose information is contained in the system.

**Mitigation:** The Department of Veterans Affairs is careful to only collect the information necessary to identify the parties involved in an incident, identify potential issues and concerns, and offer assistance to the affected parties so that they may find the help they need to get through their crisis. By only collecting the minimum necessary information, the VA is better able to protect an individual's information.

## Section 2. Uses of the Information

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

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

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

Name: Veteran's identification.
Social Security Number (SSN): used to verify Veteran identity and as a file number for Veteran.
Date of Birth: Used to confirm Veteran identity.
Mailing Address: Used to correspond with Veteran.
Zip Code: Part of the mailing address.
Phone Number: Used to correspond with Veteran.
Email Address: Used to correspond with Veteran.
Orders: Purchase Card Orders.
Charges and Reconciles: Used to verify authorized purchases.
Transfers: Accounting information.
Check Lists: Simple list of items purchased.
Reconcile Approvals: Approval of authorized purchase.
Card Management: Used to track the physical credit card.
Accrual Creation: Used for audit trails.

**2.2 What types of tools are used to analyze data and what type of data may be produced?**

*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.*

*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.*
*This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information*

• Microsoft SQL Server 2014 – SQL Server 2014 Reporting Services is used to host application reporting.

• Microsoft .Net Framework 4.0 – The .Net framework is Microsoft's premier enterprise development platform. All core business and application logic is built using the Microsoft .Net framework.

• ASP.Net – All user interfaces into the CAATS system are web based and leverage Microsoft's ASP.Net web application platform. The CAATS internal site uses traditional web forms and the external uses the ASP.Net MVC 3.0 framework.

• Internet Information Services (IIS) – The web application is hosted on load-balanced Microsoft IIS servers.

• SQL Server Reporting Services – SQL Server reporting services is leveraged to provide highly available reporting to the CAATS application. CAATS currently uses SSRS 2014.

• Developer Express (DevExpress) Web Components – CAATS uses developer express User Interface (UI) components to deliver a rich web UI experience as well as some operational reporting to end users. DevExpress components are used in both the web forms and MVC web sites.

• AJAX Control Toolkit – The CAATS team has constructed uses several custom web controls which leverage the AJAX Control Toolkit. These controls are used throughout the CAATS internal web forms application.

• NHibernate Object Relational Mapper (ORM) – NHibernate is the premier open-source object relational mapper built on the .Net framework and is used for object persistence operations. CAATS is currently using NHibernate 3.x.

• Log4Net – Standard application logging and some error logging (primarily in the Windows service) leverage Log4Net.

• ELMAH – For standard web application logging and error, CAATS uses ELMAH (Error Logging Modules and Handlers).

• StructureMap – Inversion of control (IOC) container used to implement the dependency injection pattern in CAATS. The IOC container serves both as a service locator and as a mechanism of coupling concrete class implementations to abstract interfaces at runtime.

**2.3 How is the information in the system secured?**

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

Data in transit is transmitted between system using Secure File Transfer Protocols (SFTP).

Data at rest is stored per memo FIPS 140-2 Validated Full Disk Encryption (FOE) for Data at Rest in Database Management Systems (DBMS). The OnTap storage system (NetApp AFF700) is fully FIPS 140-2 encryption compliant and meets the VA6500 requirements for data at rest encryption.

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

No.

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

Access to the application is restricted via role-based permissions. Personnel must be authorized by their supervisor, submit VA Form 8824H, and inactive accounts are disabled after 90 days.

*This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest*

**2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u> How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?**

*Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. <u>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.</u>*

*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?*

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

CAATS provides training to users, initially, and once trained there is an access process that must be submitted for individuals wanting or needing access. CAATS access form is submitted to the CAATS administrators using a VA mailbox or VA SharePoint. CAATS administrators review the form for accuracy and validity. If there are any discrepancies, the approver is notified and asked to submit a corrected form. For example, a user requesting a role of an initiator and approver for the payment module is not allowed.
The minimum-security requirements for CAATS high impact system cover 17 security-related areas regarding protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facilities employ all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives. VA Records Management Policy and the VA Rules of Behavior in Talent Management System (TMS) govern how Veterans' information is used, stored, and protected.

## 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*

Name: Veteran's identification.
Social Security Number (SSN): used to verify Veteran identity and as a file number for Veteran.
Date of Birth: Used to confirm Veteran identity.
Mailing Address: Used to correspond with Veteran.
Zip Code: Part of the mailing address.
Phone Number: Used to correspond with Veteran.
Email Address: Used to correspond with Veteran.
Orders: Purchase Card Orders.
Charges and Reconciles: Used to verify authorized purchases.

Transfers: Accounting information.
Check Lists: Simple list of items purchased.
Reconcile Approvals: Approval of authorized purchase.
Card Management: Used to track the physical credit card.
Accrual Creation: Used for audit trails.

**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. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?*

*The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.*
*This question is related to privacy control DM-2, Data Retention and Disposal.*

CAATS policy is to retain information for no longer than 6 years, 1 month, and 1 day in accordance with RCS 10-1 link for VHA: http://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

**3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.**

*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.*

RCS 10-1 link for VHA: http://www.va.gov/vhapublications/rcs10/rcs10-1.pdf. These records are retained and disposed of in accordance with the General Records Schedule (GRS) 5.1 & 5.2, approved by National Archives and Records Administration (NARA). http://www.archives.gov/records-mgmt/grs/grs20.html.

**3.4 What are the procedures for the elimination of SPI?**

*Explain how records are destroyed or eliminated at the end of the 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*

CAATS records are electronically kept, and any papers records are shredded on-site.
When the system is retired, the hard drives (and the data on them) will be destroyed in accordance with VA Handbook 6500.1 – Media Sanitization, which states that data with a security categorization of high must be destroyed. This directive defines destruction as "…the ultimate form of sanitization. After media are destroyed, they cannot be reused as originally intended. Physical destruction can be accomplished using a variety of methods including disintegration, incineration, pulverizing, shredding and melting." VA currently has a national contract (VA118-12-R-0224) with Intelligent Decisions for electronic media sanitization and destruction that requires the vendor to furnish a certificate of destruction. In the event that any drive-in use needs to be replaced for whatever reason, the contract stipulates that VA will retain the failed drives for disposal by Intelligent Decisions in accordance with the aforementioned VA directive and national contract.

**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. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?*
*This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research*

The application is not used for research. Testing and training environment does not use real data, actual PII information is restricted to the Production environment.

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

*Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.*

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

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

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

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

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

**Mitigation:** To mitigate the risk posed by information retention, CAATS adheres to Department of Veterans Affairs Records Control Schedule 10-1 (RSC 10-1). When the retention date is reached for a record, the individual's information is carefully disposed of by the determined method as described in RSC 10-1.

## 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*** |
|---|---|---|---|
| Financial Management System (FMS) | Accounting transactions used to update the accounting system record FMS | Obligations, Payments, Cost Suspense Transfers, Accounts Receivables and Budget Transactions | Secure File Transfer Protocol (SFTP |
| Credit Card System (CCS) | Purchase Card Charge Information | Purchase Card Charge and data | SFTP |
| Electronic Contracting Management System (eCMS) | Purchase Request Data | Orders, Charges, and Reconciles, Transfers, Check Lists, Reconcile Approvals, Card Management, Accrual Creation | SFTP |
| | | | |

**4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure**

*Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks.*
*This question is related to privacy control UL-1, Internal Use.*

Follow the format below:

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

**Mitigation:** The principle of need-to-know is strictly adhered to for CAATS personnel. Only personnel with a clear business purpose are allowed access to the system and the information contained within.
Users request access via VA Form 8824 indicating station, roles, and modules for which they need access.

Users are reviewed and recertified for access via a two-fold process:
• 90-day lockout. A user account without a successful login for 90 days is automatically disabled via a nightly run script.
• Annual recertification of approval roles to mirror station delegation of authority rules.

## 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*** | ***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*** | ***List the method of transmission and the measures in place to secure data*** |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| | ***with the specified program office or IT system*** | | ***use, etc. that permit external sharing (can be more than one)*** | |
| N/A | N/A | N/A | N/A | N/A |
| | | | | |

**5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure**

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

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

Follow the format below:
**Privacy Risk:** N/A.

**Mitigation:** N/A.

## 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 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?**

*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. If notice was provided in the Federal Register, provide the citation.*

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

*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. This question is 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.*

CAATS does not provide notice to individuals regarding collection of information. Information collected and stored in the system is provided by VA employees, Contractors, and Vendors as it relates to providing requested services and providing financial accounting.
The Department of Veterans Affairs does provide public notice that the system does exist. This notice is
provided in 2 ways:

1) The System of record Notice (SORN) "Personnel and Accounting Integrated Data System - VA'' (27VA047) dated 07/02/2012. The SORN can be found online at: https://www.govinfo.gov/content/pkg/FR-2012-07-02/pdf/2012-16167.pdf .

2) This Privacy Impact Assessment (PIA) also serves as notice of the Centralized Administrative Accounting Transaction System (CAATS). As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."

**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*

N/A. System information is provided from other systems. Information for the opportunity and right to decline to provide information would be covered under the other system's PIA.

**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*

N/A. System information is provided from other systems. Information for the consent for particular uses would be covered under the other system's PIA.

**6.4 PRIVACY IMPACT ASSESSMENT: Notice**

*Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.*

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

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

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

Follow the format below:
**Privacy Risk:** There is a risk that members of the public may not know that the CAATS system exists within the Department of Veterans Affairs.

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

## Section 7. Access, Redress, and Correction

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

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

*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.*

*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).*

*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.*
*This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.*

Access to working areas where information is maintained in VA facilities and VA Central Office is controlled and restricted to VA employees and VA contractors on a need-to-know basis. All users of CAATS are required to complete annual information system security training provided via the Talent Management System (TMS). Members of the public are not allowed access to CAATS. An individual who wishes to determine whether a record is being maintained under his or her name in CAATS or wishes to determine the contents of such records should submit a written request or apply in person to the VA facility where the records are located.
Users (VA employees, contractors, and vendors) must register using VA Form 8824i to gain access to CAATS. The information within CAATS is accounting data used to track funding.

**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.*

Under the jurisdiction of VHA, VHA Handbook 1605.1 Appendix D 'Privacy and Release Information', section 8 states the rights of the Veterans to amend to their records via submitted VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement, which includes designated record sets, as provided in 38 CFR 1.579 and 45 CFR 164.526. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

**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.*

CAATS is not designed for veterans to access information directly. Information requests must come from a VBA representative.

**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.*
*This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.*

*Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.*

An individual wishing to obtain more information about access, redress and record correction of Centralized Administrative Accounting Transaction System should contact the Department of Veteran's Affairs Regional Office at 1-800-827-1000. Veterans Services Representatives are available from 7:00 AM to 7:00 PM (Eastern Time), Monday thru Friday, except for federal holidays. For more information – see http://www.vba.va.gov/ro/philly/contact.htm

**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.*

*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:** Veterans cannot directly access the system. There is a risk that individuals may seek to access or redress records about them held by the VA Office and become frustrated with the results of their attempt.

**Mitigation:** Individuals may follow procedures listed in section 7.1. By publishing this PIA, and the applicable SORN, the VA makes the public aware of the unique status of applications and evidence files, such as those stored on the VA's virtualized computer systems. Furthermore, this document and the SORN provide the point of contact for members of the public who have questions or concerns about applications and evidence files as referenced in section 7.2.

## 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?**

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

*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?*

*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.*

*This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.*

Per VA Directive and Handbook 6500.1, every 5 years the Office of Information Technology (OIT) develops, disseminates, and reviews/updates a formal, documented policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; along with formal, documented procedures to facilitate the implementation of the control policy and associated controls.

OIT documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and retains individual training records for 7 years. This documentation and monitoring is performed using TMS.

Users of VA/VBA information systems gain access through a VA LAN control domain. The VA LAN uses Group Policy Objects (GPO) to manage accounts. GPO is a set of rules which control the working environment of user accounts and computer accounts. GPO provides the centralized management and configuration of operating systems, applications, and users' settings in an Active Directory environment. GPO restricts certain actions that may pose potential security risks.
Access to CAATS is granted through Common Security Services (CSS). Access is granted through the use of VA Form 8824i– CAATS Contractor Access Request Form.

**8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?**

*If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII.*

*This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

Yes, contractors will have access to the system. The access is verified through VA Vocational Rehabilitation and Employment (VR&E) personnel before access is granted to any contractor. Contracts are reviewed annually at a minimum. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via the VA's TMS. All contractors are cleared using the VA background investigation process and must obtain a Moderate Background Investigation (MBI).

**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.*

Users are required to complete information system security training activities including basic security awareness training and specific information system security training. The training records are retained for 7 years. This documentation and monitoring is performed through the use of the TMS.

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

*If Yes, provide:*

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

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

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

Yes, the Security Plan Status is current at March 04, 2024, and an Authority To Operate was granted on March 26, 2021 for 3 years expiring March 3, 2024.
The Risk Review Completion Date is September 9, 2021
The FIPS 199 classification of the system is HIGH (confidentiality=Moderate, integrity=Moderate, availability=High).

## 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).*

*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.*

No

**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)**

*This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

No

**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

**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

**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

## Section 10. References

Summary of Privacy Controls by Family

*Summary of Privacy Controls by Family*

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

| ID | Privacy Controls |
|---|---|
| UL-1 | Internal Use |
| UL-2 | Information Sharing with Third Parties |

**Signature of Responsible Officials**

**The individuals below attest that the information provided in this Privacy Impact Assessment is true and accurate.**

Tonya L. Facemire 234776

Digitally signed by Tonya L. Facemire 234776
Date: 2022.04.06 15:37:32 -04'00'

**Privacy Officer, Tonya Facemire**

Jason A Beard 202593

Digitally signed by Jason A Beard 202593
Date: 2022.04.21 10:02:22 -05'00'

**Information Systems Security Officer, Jason Beard**

James K. Ervin 580642

Digitally signed by James K. Ervin 580642
Date: 2022.04.06 12:55:09 -04'00'

**Information Systems Owner, James Ervin**

## 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).

The System of record Notice (SORN) "Personnel and Accounting Integrated Data System - VA'' (27VA047) dated 07/02/2012. The SORN can be found online at:
https://www.govinfo.gov/content/pkg/FR-2012-07-02/pdf/2012-16167.pdf