Privacy Impact Assessment for the VA IT System called:

Centralized Administrative Accounting Transaction System (Cloud) (CAATS)

Infrastructure Operations Support (IO-AS)

Veterans Affairs Central Office (VACO)

Date PIA submitted for review:

09/18/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Gina Seifert	Gina.siefert@va.gov	(202) 632-8430
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

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:

1 General Description

A. The IT system name and the name of the program office that owns the IT system.

System Name: Centralized Administrative Accounting Transaction System (Cloud) (CAATS)
Program Office: Infrastructure Operations Support (IO-AS)

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

The application provides comprehensive financial support services to VA and directly impacts Veterans' daily lives in the following ways:

- The application supports our Paralympic Veterans by directly paying them (monthly) to practice and compete.
- 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.
• 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

C. Indicate the ownership or control of the IT system or project.
VA owned and VA operated.

2. Information Collection and Sharing

D. The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
290,000. Affected individuals are service-connected disabled Veterans.

E. A general description of the information in the IT system and the purpose for collecting this information.
CAATS contains financial transaction information impacting Veteran's daily lives through support for Paralympic training/competition, Office of Transition and Economic Development (OTED) payments, Vocational services, child support payments, and purchase of grave liners.

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

G. Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.
The system is operated on one site; the VAEC Azure Government Cloud in Virginia.

3. Legal Authority and SORN

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

SORN 27VA047/ 77 FR 39346 Personnel and Accounting Integrated Data System-VA https://www.govinfo.gov/content/pkg/FR-2012-07-02/pdf/2012-16167.pdf

SORN 42VA41 Veterans and Dependents National Cemetery Interment Records-VA (Published prior to 1995) https://www.oprm.va.gov/docs/sorn/SORNsPriorto1995.PDF

SORN 58VA21/22/28/86FR61858 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

SORN 138VA005Q/74R37093 Veterans Affairs/Department of Defense Identity Repository (VADIR)-VA https://www.govinfo.gov/content/pkg/FR-2009-07-27/pdf/E9-17776.pdf

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

The system is not being modified. The system is rehoming from Austin Information Technology Center (AITC) to the VA Enterprise Cloud (VAEC) Azure Government Cloud. Current SORN's will not require revision or admendment.

D. System Changes

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

No changes to business process will result from the completion of this PIA.

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

No changes to technology will result from the completion of this PIA.

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?

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

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☒ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers*
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☐ Medical Records
- ☐ Race/Ethnicity

☐ Tax Identification Number
☐ Medical Record Number
☐ Gender
☐ Integrated Control Number (ICN)
☐ Military History/Service Connection
☐ Next of Kin
☒ Other Data Elements (list below)

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 (Servers/Database)

Centralized Administrative Accounting Transaction System (Cloud) consists of one key component (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Centralized Administrative Accounting Transaction System (Cloud) and the reasons for the collection of the PII are in the table below.

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

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
CAATS 3	Yes	Yes	Name, SSN, DoB, Mailing Address, Zip Code, Phone Number, Email address	Used to create referral order	Secure File Transfer Protocol (SFTP)

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

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?

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?

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

The Centralized Administrative Accounting Transaction System (CAATS) conducts data verification upon data entry using field verification. For example: social security numbers are limited to numeric characters only and must be nine (9) characters in length in the format XXX-XX-XXXX, Date of birth is validated using date format. Data is checked for accuracy at time of entry, for each entry.

1.4b If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

The system does not use a commercial aggregator.

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.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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.

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?

• Microsoft SQL Server 2019 – SQL Server 2019 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 2019.

• 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 at rest and in transit is encrypted.

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

System database secured via FIPS 2.0 encryption. User access is limited and approved by supervisors using VA form 8824i. Users who have not logged on for more than 90 days have their accounts deactivated by a script that runs daily.

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

All data in use, at rest, and in transit including PII/PHI is encrypted.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

2.4a How is access to the PII determined?

CAATS provides training to users, initially, and once trained there is an access process that must be submitted for individuals needing access. CAATS access form (VA Form 8824i) 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.
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.

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

Yes, VA Form 8824i.

2.4c Does access require manager approval?

Yes.

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

Yes, users are reviewed and recertified for access via a two-fold process:
a) 90-day lockout. A user account without a successful login for 90 days is automatically disabled via a nightly scan.
b) Annual recertification of approval roles to mirror station delegation of authority rules.

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

Application administrators.

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?

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?

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)?

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

RCS 10-1 link for VHA: http://www.va.gov/vhapublications/rcs10/rcs10-1.pdf.

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

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 or transfer of SPI?

Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction.
https://www.va.gov/vapubs/search_action.cfm?dType=1FMS

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

The application encrypts the SSN and claim number in the database for the Contract Exam module. 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 PRIVACY IMPACT ASSESSMENT: Retention of information

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?

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	Name, SSN, DoB, Mailing address, Zip Code, Phone number, email address	Secure File Transfer Protocol (SFTP)

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*
Credit Card System (CCS)	Purchase Card Charge information	Name, SSN, DoB, Mailing address, Zip Code, Phone number, email address	Secure File Transfer Protocol (SFTP)

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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.

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.

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	*List the purpose of information being shared / received / transmitted with the*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system*	*List the legal authority, binding agreement, SORN routine use, etc.*	*List the method of transmission and the measures in place to secure data*

	specified program office or IT system		***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

Privacy Risk: There is no external sharing of data.

Mitigation: There is no external sharing of data.

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

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:

SORN 27VA047/ 77 FR 39346 Personnel and Accounting Integrated Data System-VA https://www.govinfo.gov/content/pkg/FR-2012-07-02/pdf/2012-16167.pdf

SORN 42VA41 Veterans and Dependents National Cemetery Interment Records-VA (Published prior to 1995) https://www.oprm.va.gov/docs/sorn/SORNsPriorto1995.PDF

SORN 58VA21/22/28/86FR61858 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

SORN 138VA005Q/74R37093 Veterans Affairs/Department of Defense Identity Repository (VADIR)-VA https://www.govinfo.gov/content/pkg/FR-2009-07-27/pdf/E9-17776.pdf

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

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?

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

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?

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

Individuals do not have access to information contained in CAATS.

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

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.

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

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

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

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

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

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?

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.***

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?

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system.

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.

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

No other agencies have access to CAATS. CAATS users are granted access using VA Form 8824i.

8.1c Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

- Initiator: allows the users to input/edit transactions in the system.
- Approver: allows users to approve transactions in the system.
- Finance Approver: allows the users to perform second level review of transactions.
- Setup Admin: allows the users to setup certain back-end table need for a particular process such as purchase card data needed for the purchase card reconciliation process.

- Auditor: allows the users to perform purchase card audits in the system. No input ability.
- Report: allows the users to view reports only. No input ability.
- Read only: allows the users to view transactions only. No input ability.

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?

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 Talent Management System (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?

Yes

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved, Mar 21, 2022
2. *The System Security Plan Status Date:* Approved, Jun 20, 2023
3. *The Authorization Status:* In progress
4. *The Authorization Date:* In progress
5. *The Authorization Termination Date:* In progress
6. *The Risk Review Completion Date:* Approved, Sep 6, 2022
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

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

Section 9 – Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

Yes, CAATS Cloud is hosted in VAEC Azure GovCloud which is a FedRAMP High authorized.

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).

Yes, Infrastructure as a Service (IaaS) model

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

CAATS Cloud is hosted in VAEC Azure and is covered under the VAEC Enterprise Contract, NNG15SD22B VA118-17-F-2284

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?

No ancillary data is collected.

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

N/A.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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.

GINA SIEFERT Digitally signed by GINA SIEFERT
Date: 2023.10.02 10:20:26 -05'00'

Privacy Officer, Gina Seifert

JASON BEARD Digitally signed by JASON BEARD
Date: 2023.10.02 09:28:48 -05'00'

Information Systems Security Officer, Jason Beard

JAMES ERVIN Digitally signed by JAMES ERVIN
Date: 2023.10.02 08:05:19 -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).

SORN 27VA047/ 77 FR 39346 Personnel and Accounting Integrated Data System-VA https://www.govinfo.gov/content/pkg/FR-2012-07-02/pdf/2012-16167.pdf

SORN 42VA41 Veterans and Dependents National Cemetery Interment Records-VA (Published prior to 1995) https://www.oprm.va.gov/docs/sorn/SORNsPriorto1995.PDF

SORN 58VA21/22/28/86FR61858 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

SORN 138VA005Q/74R37093 Veterans Affairs/Department of Defense Identity Repository (VADIR)-VA https://www.govinfo.gov/content/pkg/FR-2009-07-27/pdf/E9-17776.pdf

HELPFUL LINKS:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

VA Privacy Service Privacy Hub:

https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices