Privacy Impact Assessment for the VA IT System called:

PHILADELPHIA INFORMATION TECHNOLOGY CENTER COURSEWARE DELIVERY SYSTEM (PITC CDS)

Veterans Benefit Administration

Office of Human Capital Services (HCS)

Date PIA submitted for review:

10/05/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Jason Anderson	Jason.Anderson3@va.gov	202-570-0255
Information System Security Officer (ISSO)	Jose Diaz	Jose.Diaz@va.gov	312-980-4215
Information System Owner	Daniel Desormeaux	daniel.desormeaux@va.gov	407-835-5552

Abstract

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

The Courseware Delivery System (CDS), owned by the VBA Office of Human Capital Services (HCS), is a web-based application that supports VBA training initiatives viewed through a shared interface. CDS provides uniform and consistent training to employees in all VA Regional Offices, to improve the accuracy and consistency of Veterans' claims processing nationwide. It supports application and training courses(content) which are completed by VBA employees as part of their annual training requirements. CDS does not access or pull information from other VBA applications which contain Veteran claims information.

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.

The Philadelphia Information Technology Center Courseware Delivery System (PITC CDS), owned by the VBA Human Capital Services (HCS) is a web-based application that supports VBA training initiatives viewed through a shared interface. PITC CDS supports uniform and consistent training to approximately 22,000 employees (including contractors) in all VA Regional Offices, to improve the accuracy and consistency of Veterans' claims processing nationwide. It supports application and training courses (content) which are completed by VBA employees as part of their annual training requirements. PITC CDS does not access or pull information from other VBA applications which contain Veteran claims information. PITC CDS stores VBA training course progress information for employees.

Education Data Repository (EDR) and Talent Management System (TMS) share information internally with PITC CDS. There is a database link between PITC CDS and Education Data Repository (EDR) to retrieve employee information. The Talent Management System (TMS) is the official system of records for all VA employee training information and provides training assignment information to PITC CDS for PITC CDS hosted training content. PITC CDS utilizes TMS Web Services to supply TMS with completion information for the PITC CDS hosted training content.

TMS also shares VBA historical training information via secure file transfer protocol (sFTP) with PITC CDS which is then provided to the VBA Enterprise Data Warehouse (EDW). There is database link that EDW utilizes to access the VBA historical training information.

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

The Philadelphia Information Technology Center Courseware Delivery System (PITC CDS), owned by the VBA HCS office is a web-based application that supports VBA training initiatives viewed through a shared interface. CDS provides uniform and consistent training to employees in all VA Regional Offices, to improve the accuracy and consistency of Veterans' claims processing nationwide. It supports application and training courses(content) which are completed by VBA employees as part of their annual training requirements. CDS does not access or pull information from other VBA applications which contain Veteran claims information.

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

Human Capital Services

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.

PITC CDS supports uniform and consistent training to approximately 22,000 employees (including contractors) in all VA Regional Offices, to improve the accuracy and consistency of Veterans' claims processing nationwide. It supports application and training courses (content) which are completed by VBA employees as part of their annual training requirements.

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

PITC CDS supports application and training courses (content) which are completed by VBA employees as part of their annual training requirements. PITC CDS does not access or pull information from other VBA applications which contain Veteran claims information. PITC CDS stores VBA training course progress information for employees.

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

Education Data Repository (EDR) and Talent Management System (TMS) share information internally with PITC CDS. There is a database link between PITC CDS and Education Data Repository (EDR) to retrieve employee information. The Talent Management System (TMS) is the official system of records for all VA employee training information and provides training assignment information to PITC CDS for PITC CDS hosted training content. PITC CDS utilizes TMS Web Services to supply TMS with completion information for the PITC CDS hosted training content.

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 application is operated only at Philadelphia Information Technology Center.

3. Legal Authority and SORN

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

The Secretary of Veterans Affairs established these guidelines pursuant to the authorities in and requirements of Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled 'Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C 51 535), titled 'Agency Agreements," also known as the "Economy Act." These guidelines assist in the implementation of these statutes. SSN serves as unique identifier for record retrieval of the Veteran. The legal authority is Executive Order 9397, which allows the collection and use for business purposes/enrollment and 32 CFR 505.4(a) (b) for individual's rights, benefits, and privileges under federal programs. SORN 76VA05 General Personnel Records (Title 38).

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?

There is no modification to the system right now.

D. System Changes

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

No.

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

No.

Section 1. Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

1.1 What information is collected, used, disseminated, created, or maintained in the system?

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.
This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1.

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

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

- Last Name
- First Name
- Email Address
- Student ID
- VA State Code and or VA Identification Number.>.

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

PII Mapping of Components (Servers/Database)

Philadelphia Information Technology Center Courseware Delivery System (PITC CDS) consists of two e key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by PITC CDS 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
CDS, VALMS	Yes	Yes	Employee Name, TMS Student Identification, and email address, VA state code and VA Identification number	CDS uses this information to track training enrollment and progress for CDS courses	Data is encrypted
CDSTMS	Yes	Yes	VBA Employees (only): Employee Name, TMS Student Identification, and email address.	CDS uses this information to track training enrollment and progress for CDS courses	Data is encrypted.

1.2 What are the sources of the information in the system?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

PITC CDS receives the TMS Student Identifier when a PITC CDS course is launched from TMS. PITC CDS then queries the Education Data Repository (EDR) database to retrieve the employee's full name, TMS Student Identifier and email address, if the TMS Student Identifier has not already been imported into PITC CDS. PITC CDS does not collect data directly from the individual employee; all data is collected electronically through interfaces:

- Education Data Repository (EDR)
- Talent Management System (TMS)
- Enterprise Data Warehouse (EDW)

FOR MEMBERS OF THE PUBLIC:

Every VA provided training courses accessed by members of the public provides a registration automated form which collects the necessary information (email address, VA state code, and VA assigned identification number (when applicable) from members of the public and stores in the CDS database.

1.2b Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

The CDS application is only accessible by internal VA employees and contractors. Access has to be approved by the System Owner and access uses VA Active Directory login username to determine access. No other sources are used to determine access. For VA Employees who take training courses, user information is retrieved from the Talent Management System (TMS) which is the VA System of Record. For Members of the Public, information is gathered directly from the individual. No additional sources are used.

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

The system does not create any information.

1.3 How is the information collected?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

PITC CDS only collects information from the Education Data Repository (EDR) system using a database link. PITC CDS does not collect data directly from the individual employee. PITC CDS receives the Sensitive Personal Information (SPI) information identified in 1.1 directly from the EDR for VBA employees who launch TPSS training from TMS. The interface between the EDR and PITC CDS transfers data (1) when a new student record needs to be created in PITC CDS and (2) when an existing PITC CDS student's record needs to be updated to match the corresponding EDR data. This synchronization occurs during a regularly scheduled nightly process or if there is an issue with a PITC CDS application user. All data are collected electronically.

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

This is not applicable to PITC CDS. Since, all data are collected electronically.

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.

PITC CDS has a nightly interface with the EDR which is used to ensure the SPI data stored in PITC CDS matches the data imported from EDR. In addition, the PITC CDS support application includes an on- demand update function for updating the SPI data. Interconnection Security Agreements (ISAs) and Interface Control Documents (ICDs) document the interfaces between CDS, EDR, TMS, and EDW.

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.

PITC CDS receives data from the VA System of Records or the individual, so CDS does not perform any accuracy checks or use any commercial aggregator of information.

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

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

The Secretary of Veterans Affairs established these guidelines pursuant to the authorities in and requirements of Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency Agreements," also known as the "Economy Act." These guidelines assist in the implementation of these statutes.

1.6 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (*Work with your System ISSO to complete this section)*

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: There is a risk of losing training progress data or loss of integrity of data that would adversely affect capturing employee training activity and completions accurately in the VA system of records for training (VA TMS).

Mitigation: CDS includes error trapping functions when transmitting training progress and training completions to the TMS. The errors are reviewed weekly and re-transmitted as needed. Additionally, CDS maintains historical enrollment/training progress data. Training enrollments and progress data are transferred to the historical archives nightly.

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.

PITC CDS purpose is to provide uniform and consistent training to employees in all VA Regional Offices to improve the accuracy and consistency of Veterans' claims processing nationwide. PITC CDS usage of the SPI information ensures the VA TMS data accuracy, as well (i.e., the appropriate TMS Student Identifier receives completion credit).

- Employee name: Used to display name in the training course user interface.
- Talent Management System (TMS) Student Identifier: Used as an identifier to identify student.
- Email address: Used by support team to identify user.
- VA State code: used to report external student results by state.

- VA Identification number: used to authorize access to external training.

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.

PITC CDS does not perform any type of analysis of individual training records. It provides data to TMS which is used to analyze individual employee training records. PITC CDS does generate usage reports which are used to determine effectiveness of the PITC CDS application. Usage reports include the number of completions per month per course.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

PITC CDS does not perform any type of analysis of individual training records. It provides data to TMS which is used to analyze individual employee training records. Usage Reports are generated to determine the effectiveness of the PITC CDS Training courses. Usage reports are reported at the course level; no new information relating to the individual is created.

2.3 How is the information in the system secured?
These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

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

Data in transit uses secure communication protocols (HTTPS) to encrypt data communication to the PITC CDS servers. Database connection information is protected by using the RSA Protected Configuration Provider class. Data at rest is encrypted using SQL Server database encryption.

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

PITC CDS is not storing Social Security Numbers.

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

Data in transit uses secure communication protocols (HTTPS) to encrypt data communication to the PITC CDS servers. Database connection information is protected by using the Rivest Shamir Algorithm (RSA) Protected Configuration Provider class. Data at rest is encrypted using SQL Server database encryption.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. ***Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.***

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

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

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

2.4a How is access to the PII determined?

Only PITC CDS application users are allowed access to the SPI information and these users are required to complete a background check and to annually complete the VA Cybersecurity and Privacy training. Individuals who complete PITC CDS hosted training content are not allowed access to the PITC CDS application or SPI information.

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

Yes

2.4c Does access require manager approval?

Yes

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

Yes

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

The system owner is responsible for assuring PII protection.

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

PITC CDS does not access or pull information from other VBA applications which contain Veteran claims information. PITC CDS only retains names, email addresses, TMS Student ID, and VBA training course progress information. This data must be retained to verify employees who have utilized training resources in the past. The SPI data collected is integral to the VA's ability to identify employees who have utilized training resources in the past. PITC CDS retains training enrollment and progress data indefinitely but does archive completed training enrollment and progress data to a historical data store nightly.

3.2 How long is information retained?

*In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. **For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods**. The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented. If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

PITC CDS does not access or pull information from VBA applications which contain Veteran claims information. The data retention period for employee training records in PITC CDS is 5 years. VBA must be able to verify which training resources have been used by employees in the past. PITC CDS does archive completed training enrollment and progress data to a historical data store nightly.

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

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner. Please work with the system Privacy Officer and VA Records Officer to answer these questions.
This question is related to privacy control DM-2, Data Retention and Disposal.

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

GENERAL RECORDS SCHEDULE 5.2 Transitory and Intermediary Records- 020 Intermediary records. They exist for the sole purpose of creating a subsequent record and They are not required to meet legal or fiscal obligations, or to initiate, sustain, evaluate, or provide evidence of decision-making. This includes certain analog and electronic source records for electronic systems that are not otherwise excluded. Temporary Destroy upon creation or update of the final record, or when no longer needed for business use, whichever is later. The GRS provides disposition authority for electronic records from one system that are used as source records to another system. The GRS does not apply to either the originating system or the final system in which the final records reside. Since TMS is the official System of Record, this disposition does not change the disposition currently used for TMS. PITC CDS is not the system of record for training records. TMS is the system of record and would be responsible for data retention policy. No record is stored in PITC CDS.

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

GENERAL RECORDS SCHEDULE 5.2 Transitory and Intermediary Records- 020 Intermediary records. They exist for the sole purpose of creating a subsequent record and They are not required to meet legal or fiscal obligations, or to initiate, sustain, evaluate, or provide evidence of decision-making. This includes certain analog and electronic source records for electronic systems that are not otherwise excluded. Temporary. Destroy upon creation or update of the final record, or when no longer needed for business use, whichever is later. The GRS provides disposition authority for electronic records from one system that are used as source records to another system. The GRS does not apply to either the originating system or the final system in which the final records reside. Since TMS is the official System of Record, this disposition does not change the disposition currently used for TMS. PITC CDS is not the system of record for training records. PITC CDS is not the system of record for training records. TMS is the system of record and would be responsible for data retention policy. No record is stored in PITC CDS.

3.4 What are the procedures for the elimination or transfer of SPI?

Explain how records are destroyed, eliminated or transferred to NARA at the end of their mandatory retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.? This question is related to privacy control DM-2, Data Retention and Disposal.

Data is not eliminated. It is controlled in accordance with NARA control schedules determined by agency involved. VA Handbook 6300.1 Records Management Procedures explains the Records Control Schedule procedures. Operating units will follow VA policy.

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

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

PITC CDS information is not used for testing, training, or research purposes.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

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

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

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

Follow the format below:

Privacy Risk: As described herein, support systems retain information until that work in progress is completed and data is committed to master systems and records. The master systems retain data on a permanent basis (beyond the termination of an employee). If a master system is to be deactivated, critical information is migrated to the new system and the old system along with associated data is archived according to the application disposition worksheet. As such, SPI, PII or PHI may be held for long after the original record was required to be disposed. This extension

of retention periods increases the risk that SPI, PII or PHI may be breached or otherwise put at risk.

Mitigation: VA TMS is the system of records for training records for VA employees and allows retrieval of record via personal identifier. CDS is the course content hosting system which presents training course content and tracks training progress. CDS only collects the necessary information (Student name, TMS Student ID, and email address) that is required to accurately identify an employee to the TMS system. CDS does not collect all information available for an employee.

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***
Education Data Repository (EDR)	To retrieve the employee information (employee name information (last name, first name)	Employee name information (last name, first name), TMS, Student ID, email address.	Database link between CDS and EDR
Talent Management System (TMS)	TMS is the official system of records for all VA employee training information	TMS Student ID and course completion information	TMS Web Services and Secure FTP
Enterprise Data Warehouse (EDW)	Pertinent Personally Identifiable Information (PII) that is required to accurately identify a VA employee or VA contractor	Employee name information (last name, first name), TMS Student ID, email address	Database Link between CDSTMS and EDW

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: There is a risk that employee's specific training progress can be identified.

Mitigation: VA TMS only allows employees to access training that has been assigned by their supervisor, local training manager, or by the employee themselves. PITC CDS verifies that the employee accessing the training is a valid employee and tracks training progress by TMS student identifier. PITC CDS administrative users must complete the annual VA security and privacy training and sign the rules of behavior. TMS users also must complete the annual VA security and privacy training and sign the rules of behavior as well as to complete specific administrative training for TMS.

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.

CDS is not sharing information outside of VA.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

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

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: There is a risk that privacy information may be released to unauthorized individuals.

Mitigation: All personnel with access to PITC CDS are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually. VA TMS only allows employees to access training that has been assigned by their supervisor, local, training manager or by the employee themselves. PITC CDS verifies that the employee accessing the training is a valid employee and tracks training progress by TMS student identifier.

Section 6. Notice

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

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

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

VA TMS is the system of records for training records for VA employees. PITC CDS is the course content hosting system which present training course content and tracks training progress. VA TMS web

application provides the Privacy Policy website link at the bottom of every page displayed once a user logs into the TMS system which goes into details on what data could be collected from the end user. The Department of Veterans Affairs provides public notice that the system exists in two ways:

- The official system of records notice (SORN) 76VA05 dated July 20, 2000 citation 65FR45131 for "General Personnel Records" (Title 38)-VA can be found online at:
  http://www.gpo.gov/fdsys/pkg/FR-2000-07-20/pdf/00-18287.pdf
  https://www.oprm.va.gov/docs/Current_SORN_List_06_25_2021.pdf

- This Privacy Impact Assessment (PIA) also serves as notice of the Courseware Delivery System. 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."

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

PITC CDS requires the user to login to the VA network before access. The VA network access login process provides the notice. VA TMS is the system of records for internal VA employees. VA TMS provides the notice upon login. TMS routes student directly to the training courses. For members of the public, users login to another VA system which provides the notice. These system routes the user directly to the training course. .

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

PITC CDS is the course content hosting system which present training course content and tracks training progress. Other systems are used to access the training courses. Notice in these systems is adequate.

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.

VA TMS is the system of records for training records for VA employees. PITC CDS is the course content hosting system which present training course content and tracks training progress. VA TMS does not allow employees to opt out of training since training is an employee requirement to perform their job duties.

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.

VA TMS is the system of records for training records for VA employees. The sole use of the information is to identify individual users of PITC CDS to ensure they receive proper credit for training they have taken. VA TMS does not allow employees to opt out of training, so the employee does not have the right to consent to particular uses of their information.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

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

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

Privacy Risk: There is a risk that members of the public may not know that the Courseware Delivery 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?

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer***

satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.

Any individual wishing to obtain more information about access, redress and record correction of Courseware Delivery System should contact the Department of Veteran's Affairs regional as directed in the System of Record Notice (SORN). The official system of records notice (SORN) 76VA05 dated July 20, 2000 citation 65FR 45131 for "General Personnel Records" (Title 38)-VA can be found online at: http://www.gpo.gov/fdsys/pkg/FR-2000-07-20/pdf/00-18287.pdf

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).

TMS is the system of record as noted in the section 3.1 of the current PTA

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.

Employees must complete New Employee Orientation training which includes Privacy and Information Security training. The Employee must obtain a PIV and pass a background investigation. Once completed, the employee must obtain approval from their manager and approval from the TMPI manager for access.

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.

- An individual may request amendment of a record pertaining to themselves contained in a specific VA system of records by emailing or delivering the request to their training manager or their VA liaison. The individual must state the nature of the information in the record the individual believes to be inaccurate, irrelevant, untimely, or incomplete; why the record should be changed; and the amendment desired. The requester should be advised of the title and address of the VA official who can assist in preparing the request to amend the record if assistance is desired.

- Not later than 10 days, excluding Saturdays, Sundays, and legal public holidays, after the date of receipt of a request to amend a record, the VA official concerned will acknowledge in writing such receipt. If a determination has not been made, the acknowledgement will inform the individual when he or she may expect to be advised of action taken on the request. VA will complete a review of the request to amend or correct a record as soon as reasonably

possible, normally within 30 days from receipt of the request (excluding Saturdays, Sundays, and legal public holidays).

- Where VA agrees with the individual's request to amend his or her record(s), the record(s) will be corrected promptly, and the individual will be advised promptly of the correction. Amendment consists of adding information to the record, altering information in the record, or deleting information in the record. Under the Privacy Act, if information is altered or deleted, the previous version must be obliterated and illegible after amendment. The amendment should be annotated "Amended, Privacy Act, (date), (signature and title of amending official)."

- If the record has previously been disclosed to any person or agency, and an accounting of the disclosure was made, prior recipients of the record will be informed of the correction. FL 70-19, Notification to Other Person or Agency of Amendment to a Record, may be used.

- If it is determined not to grant all or any portion of the request to amend a record, the official will promptly notify the individual in writing. The individual will be advised of his or her righto file a concise statement of reasons for disagreeing with the refusal to amend. The notice will specify the reason(s) for denying the request, identify the VA regulations or statutes upon which the denial is based, and advise that the denial may be appealed in writing to the General Counsel (024), Department of Veterans Affairs, 810 Vermont Avenue, NW, Washington, DC 20420. FL70-20, Notification of Initial Refusal to Amend a Record under the Privacy Act, may be used for this purpose.

- The determination on an appeal will be made not later than 30 days, excluding Saturdays, Sundays, and legal public holidays, from the date the individual's letter of appeal is received unless the Secretary or Deputy Secretary, for good cause shown, extends such 30-day period. If the 30-day period is so extended, the individual will be notified promptly of the reasons for the extension and the date on which a final determination may be expected. The final determination in such appeals will be made by the General Counsel or Deputy General Counsel.

- If the General Counsel or Deputy General Counsel finds that the adverse determination should be reversed, he or she will notify the VA office or station of the remedial action to be taken. The VA office or station will promptly carry out that action. The General Counsel or Deputy General Counsel will promptly notify the individual in writing of the corrective action. The field station or Central Office organization that provided the initial decision will inform previous recipients of the record that a correction has been made.

- If the General Counsel or Deputy General Counsel determines that the adverse determination will not be reversed, the individual will be notified promptly in writing of that determination, the reasons therefor, and of his or her right to seek judicial review of the decision pursuant to section 3 of the Privacy Act (5 U.S.C. 552a(g).

- If the adverse determination is sustained by the General Counsel or Deputy General Counsel, the individual will also be advised promptly of his or her right to file a concise statement of reasons for disagreeing with the refusal to amend. The statement may contain information that the individual believes should be substituted.

- When an individual files a statement disagreeing with VA's decision not to amend a record, the record will be clearly annotated so that the fact that the record is disputed is apparent to anyone who may subsequently access, use, or disclose it. When the disputed record is disclosed to persons or other agencies, the fact of the dispute will be clearly noted. Copies of the statement of disagreement will be provided, and, when appropriate, copies of a concise statement of VA's reasons for not making the amendment(s) requested will also be provided.

- A decision by either the General Counsel or Deputy General Counsel pursuant to paragraph 3f (7) of this handbook is final. It is subject to judicial review in the district court of the United States in which the complainant resides, or has his or her principal place of business, or in which the VA records are located, or in the District of Columbia.

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.

Any individual wishing to obtain more information about access, redress and record correction of Courseware Delivery System should contact their training manager or their VA liaison. The official system of records notice (SORN) 76VA05 dated July 20, 2000 citation 65FR 45131 for "General Personnel Records" (Title 38)-VA can be found online at: http://www.gpo.gov/fdsys/pkg/FR-2000-07-20/pdf/00-18287.pdf

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

Any individual wishing to obtain more information about access, redress and record correction of Courseware Delivery System should contact their training manager or their VA liaison. The official system of records notice (SORN) 76VA05 dated July 20, 2000 citation 65FR 45131 for "General Personnel Records" (Title 38)-VA can be found online at: http://www.gpo.gov/fdsys/pkg/FR-2000-07-20/pdf/00-18287.pdf.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. ***For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.*** *(Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

Principle of Individual Participation: If access and/or correction is denied, then is the individual provided notice as to why the denial was made and how to challenge such a denial?

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?
This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk:
There is a risk that individual may seek to redress records about them held by the VA Office and become frustrated with the results of their attempt.

Mitigation:
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 Courseware Delivery System platform. 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.

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.

Per VA Directive and Handbook 6330, 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 are performed using VA TMS.

VBA Office of Human Captial Services (HCS) determines who obtains access to the CDS application and which roles are assigned based upon the user's job responsibilities.
The CDS application has 5 user roles which are:

- Administrator – Allowed to access all functions.
- Help Desk – Allowed to access all functions except for administrative functions.
- Course Advocates – Allowed to access the Item and User functions.
- Course Manager – Allowed to only access the reports (Items and Users) and Training Group functions.
- Student – Not allowed access to any of the application functions. Students must login to TMS first to access CDS hosted courses/content.

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?

PITC CDS is not typically accessible to users from other agencies. If users from other agencies were allowed access, then they would be assigned the Student User Role.

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.

The CDS application has 5 user roles which are:

- Administrator – Allowed to access all functions.
- Help Desk – Allowed to access all functions except for administrative functions.
- Course Advocates – Allowed to access the Item and User functions.
- Course Manager – Allowed to only access the reports (Items and Users) and Training Group functions.
- Student – Not allowed access to any of the application functions. Students must login to TMS first to access CDS hosted courses/content.

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

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

describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

VA contract employee access is verified through the Contracting Officer's Representative (COR) and other VA supervisory/administrative personnel before access is granted to any VA system. Contractor access is 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 Talent Management System, which contains an NDA/Confidentiality agreement to be signed upon completion. All contractors are vetted using the VA background investigation process and must obtain the appropriate level background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access. Generally, contracts are reviewed at the start of the initiation phase of acquisitions and again during procurement of option years by the Contracting Officer, Information Security Officer, Privacy Officer, COR, Procurement Requestor/Program Manager and any other stakeholders required for approval of the acquisition. Contracts generally have an average duration of 1-3 years and may have option years stipulated in the original contract.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA Privacy and Information Security Awareness and Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. Personnel is not required to complete HIPAA training since personnel does not handle Veteran claim information.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 05 Jun 2023
3. *The Authorization Status:* Authorization To Operate
4. *The Authorization Date:* Please provide response here
5. *The Authorization Termination Date:* 10 August 2025
6. *The Risk Review Completion Date:* 24 July, 2023

7. *The FIPS 199 classification of the system:* 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.***

N/A

Section 9 – Technology Usage

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

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

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

CDS does not use cloud technology

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

CDS is not using cloud technology

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.

CDS is not using cloud technology

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.

CDS is not using cloud technology

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).

CDS is not using RPA

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 they provided in this Privacy Impact Assessment is true and accurate.

JASON ANDERSON

Digitally signed by JASON ANDERSON
Date: 2023.12.20 08:41:39 -05'00'

Privacy Officer, Jason Anderson

JOSE DIAZ

Digitally signed by JOSE DIAZ
Date: 2023.12.20 10:42:59 -06'00'

Information System Security Officer, Jose Diaz

DANIEL DESORMEAUX

Digitally signed by DANIEL DESORMEAUX
Date: 2024.01.10 14:37:10 -05'00'

Information System Owner, Daniel Desormeaux

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).

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