Privacy Impact Assessment for the VA IT System called:

# VA IT Virtual Campus Assessing

# Office of Information & Technology (OIT)

# People Readiness (PR)

# eMASS ID #998

Date PIA submitted for review:

February 7, 2024

System Contacts:

*System Contacts*

| | Name | E-mail | Phone Number |
|---|---|---|---|
| Privacy Officer | Tonya Facemire | Tonya.Facemire@va.gov<br>OITPrivacy@v.gov | 202-632-8423 |
| Information System Security Officer (ISSO) | Collin Roberts | Collin.Roberts@va.gov | 432-263-7361 |
| Information System Owner | Daniel Jones | Daniel.Jones6@va.gov | 202-701-5126 |

## Abstract

*The abstract provides the simplest explanation for "what does the system do?".*

VA IT Virtual Campus Assessing has developed a web application, VA People Readiness (PR) for delivering live and on demand video training. PR incorporates a green screen studio and a web application designed by PR contractors to deliver live and on demand video training. This training covers a variety of topics to include cyber security, IT specialties, VA policy, conferences, and Senior Leadership events. The training does not include any PII or PHI material and is generic in nature. It allows for students at any VA facility or from home to attend training and interact directly with the instructor via online chat or other social media modalities. PR ensures all students are associated with the VA by using VA email accounts to verify status. We link all training to the TMS ID of students using an automatic method to give credit in TMS for courses attended.

## 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. What is the IT system name and the name of the program office that owns the IT system?*

VA IT Virtual Campus
Office of Information Technology (OIT)
Office of People Science (OPS)
People Readiness (PR)

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

People Readiness (PR) has developed a web application for delivering live and on-demand video training per Executive Order 11348 (Providing for the Further Training of Government Employees) and Executive Order 1311 (Using Technology to Improve Training Technologies for Federal Government Employees).

*C. Who is the owner or control of the IT system or project?*

People Readiness (PR)

*2. Information Collection and Sharing*

*D. What is the expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual?*

The VA IT Virtual Campus is used for all VA employees and contractors needing to satisfy VA training requirements listed in VA policy. The current number of users is 62,483.

*E. What is a general description of the information in the IT system and the purpose for collecting this information?*

The VA IT Virtual Campus is used for training purposes. The information gathered is used to apply proper credit for classes taken. Email address is used to verify participants are employed by the Department of Veterans Affairs, either as a full-time employee or contractor, and given access to the web application. TMS ID is used to ensure students are given credit for courses/events attended. IP addresses are collected for troubleshooting and performance related issues.

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

PR captures VA email addresses and TMS ID as an external system to VA and that data collection is used to provide credit for individuals training in this distance learning platform in our TMS system.

*G. Is 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?*

VA IT Virtual Campus is a cloud-based system located in Amazon AWS East, which is a FedRAMP approved environment.

*3. Legal Authority and SORN*

*H. What is the citation of the legal authority to operate the IT system?*

The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. The authority of maintenance of the system listed in question 1.1 falls under Title 28, United States Code, title 38, U.S.C., sections 501(a), 1705, 1710, 1722, and 5317.

Executive Order 11348 (Providing for the Further Training of Government Employees) and Executive Order 1311 (Using Technology to Improve Training Technologies for Federal Government Employees).

*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 in the process of being modified and a SORN does exist.

*4. System Changes*

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

There will not be a need to change any business processes as the result of this PIA.

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

There will not be a need for any technology changes because 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?**

*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. It must also match the information provided in question 3.4 of the PTA.*

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[1]

☐ 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)

Occupational, Education, Medical)

Other PII/PHI data elements: TMS ID.

**PII Mapping of Components (Servers/Database)**

VA IT Virtual Campus consists of 2 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by VA IT Virtual Campus 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 server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

*Internal Components Table*

| Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI | 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 |
|---|---|---|---|---|---|
| Database Service (AWS) | Yes | Yes | Name, IP address, TMS ID | To verify user is a VA employee and give credit | Database restrictions ensure only |
| Web Service (AWS) | Yes | Yes | Name, IP address, TMS ID | Transfers directly to database. | Only has access during account creation and upon user course completion. |

**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?*

Individual provides email address, name and TMS ID. System generated reports specifying course taken by TMS ID that is automatically transferred to the TMS system. The IP address is obtained automatically upon connection to an event to identify the connection.

*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.*

No information is gathered from other sources. All information is collected via a registration page within the application. VA IT Virtual Campus users type in the information to obtain an account. The IP address is obtained by the campus application to identify the connection.

*1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?*

The application generates various reports and renders them into Reporting Services as part of Amazon database service. Various reports can be produced for application administration purposes, such as PDF reports and web reports.

**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?*

Information is collected via a registration page within the application or through Single-Sign-On (SSOe) credentials being passed from the VA PIV card. Users who manually register, type in the information to obtain an account. The IP address is obtained by the campus application to identify the connection.

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

N/A

**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.*

TMS team verifies TMS ID for accuracy when importing data into TMS. Email verification is performed during the registration process. This is done one of two ways; if the email account is generated from a VA.gov address the application sends the user an email to that address. If the registered email address is a non-VA address, the help desk must manually activate the user account.

*1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?*

The VA IT Virtual Campus does not utilize a commercial aggregator for data accuracy.

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

The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. The authority of maintenance of the system listed in question 1.1 falls under Title 28, United States Code, title 38, U.S.C., sections 501(a), 1705, 1710, 1722, and 5317.

*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*

Per Executive Order 11348 (Providing for the Further Training of Government Employees) and Executive Order 1311 (Using Technology to Improve Training Technologies for Federal Government Employees), Email addresses and TMS user ID's are required by VA policy to be used to record all training in the TMS. TMS has been mandated for the single repository for all training documentation. PR must capture VA email addresses and TMS ID as an external system to VA and that data collection is used to provide credit for individuals training in this distance learning platform in our TMS system.

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

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

> **Privacy Risk:** Email addresses and TMS user ID's are required by VA policy to be used to record all training in the TMS. TMS has been mandated for the single repository for all training documentation. ITWD must capture VA email addresses and TMS ID as an external system to VA and that data collection is used to provide credit for individuals training in this distance learning platform in our TMS system. There is a risk that sensitive information could be access by unauthorized individuals.
>
> **Mitigation:** Individuals provide their email address and TMS ID when creating an account through our system. The information is entered through an encrypted interface on a FedRAMP approved encrypted network into an encrypted database that has been categorized to hold that level of sensitive data. Controls are in place to limit who can access the 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 that 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.*

| PII/PHI Data Element | Internal Use | External Use |
|---|---|---|
| Name | Used to verify VA employee and give course credit | Not used |
| IP Address | Troubleshooting and performance related issues | Not used |
| TMS ID | Used to give course credit to TMS | Not used |

**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?*

The application generates various reports and renders them into Reporting Services as part of Amazon database service. Various reports can be produced for application administration purposes, such as PDF reports and web reports.

*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.*

The information gathered is used for reporting completed courses and provide course credit in TMS.

### 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 is encrypted in transit and at rest and database admins are the only personnel with access to the data.

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

Social Security Numbers are not being collected.

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

The PIA states the information is used to provide credit for training taken for individuals. This information is necessary to give proper credit for training taken in the VA IT Virtual Campus. Access to the database is limited to the database admins. Training credit is given through an automated process linked directly to TMS. IP addresses are visible through a performance dashboard but that shows throughput and disconnects but are not linked to an individual's account.

### 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?*

VA employees and contractors supporting the system have access to the system to provide system technical support. Prior to being granted this access, they must complete associated Role-Based and Rules of Behavior training. This training is required and updated on an annual basis.

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

Yes. This is documented in the CMS section of the Administrator Manual.

*2.4c Does access require manager approval?*

Yes. To obtain CMS application access, the technical team sends an email to the VA IT Campus System Owner for approval and role designation.

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

Yes. Audit logs are collected and reviewed by technical support staff.

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

People Readiness technical support staff

## 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*

All registration data (name, email address, TMS ID) entered by the user or passed through SSOe, is retained in the database. All data related to student courses through the software is also retained. IP addresses are retained separately and not linked to student data.

**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.*

Records older than 7 years will be purged from the system.

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

*An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner. 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?*

Yes

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

Per the SORN office, TMS is considered the system of record for all training related completions. Once the VA IT Campus uploads (nightly) to TMS through an API, then the data is no longer necessary. We retain a course history within our database for 7 years, at which time we remove old items.

**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.*

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=1

**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.*

PII is not utilized in testing or development environments. No PII is used in any of the training materials presented.

**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.*

**Privacy Risk:** VA IT Virtual Campus only retains necessary information to give the credit for courses taken. There is a risk information could be maintained longer than necessary.

**Mitigation:** VA IT Virtual Campus follows retention schedule as outlined in the SORN.

## 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*** |
|---|---|---|---|
| Talent Management System (TMS) | Used for giving course credit | TMS ID | Automated ingest nightly through TMS plugin |
| VA People Readiness (PR) | Information about courses and students | Name, TMS ID, IP Address | Direct data extract |

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

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

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

**Privacy Risk:** Currently name and TMS ID are stored in VA IT Virtual Campus. There is a risk that unauthorized individuals may access the information.

**Mitigation:** VA IT Virtual Campus plugin for TMS directly exports data to TMS. No other entities have access to that information.

## Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

**5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?**

**Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.**

**NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.**

*Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.*

*For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.*

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

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

*Data Shared with External Organizations*

| ***List External Program Office or IT*** | ***List the purpose of information*** | ***List the specific PII/PHI data elements that are processed*** | ***List the legal authority, binding*** | ***List the method of transmissio*** |
|---|---|---|---|---|

| *System information is shared/received with* | *being shared / received / transmitted with the specified program office or IT system* | *(shared/received/transmitted) with the Program or IT system* | *agreement, SORN routine use, etc. that permit external sharing (can be more than one)* | *n and the measures in place to secure data* |
|---|---|---|---|---|
| Thunderyard Liberty JV, LLC | Contract Partner for project | Name, TMS ID, IP Address | Contract # 36C10B21D1036 | TCP/IP |
| Mantech International | Subcontractor for project | Name, TMS ID, IP Address | Contract # 36C10B21D1036 | TCP/IP |
| BAH | Subcontractor for project | Name, TMS ID, IP Address | Contract # 36C10B21D1036 | TCP/IP |

**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.*

*If no External Sharing listed on the table above,* ***(State there is no external sharing in both the risk and mitigation fields).***

*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*

**Privacy Risk:** There is a risk that unauthorized individuals may access the information. However, data is not shared outside the department.

**Mitigation:** Only authorized individuals have access to the information. There are access controls as well as audit logs in place to prevent unauthorized access.

## 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.*

Registrants are informed that information collected is considered PII by the Privacy Act of 1974. This information is required to give TMS credit for courses taken. Failure to provide the requested information will result in being denied access to the VA IT Virtual Campus web application.

*Some of the information being requested to enable registration with the VA IT Campus is considered Personally Identifiable Information (PII) by the VA Privacy Office. This information is used only to provide users TMS credit for courses completed as well as general access to and use of the Campus. Failure to provide this information will result in access being denied to the VA IT Campus. PII will not be disseminated, shared, or used for training purposes. Authorized technical staff of ITWD will be the only users with access to PII in case of request by any individual user if needed. Some technical data (IP address, network connection speed, etc.) is also being gathered for purposes of technical support.*

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

www.vaitcampus.com

*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.*

The following notice is on the login page of the VA IT Virtual Campus website:

Some of the information being requested to enable registration with the VA IT Campus is considered Personally Identifiable Information (PII) by the VA Privacy Office. This information is used only to provide users TMS credit for courses completed as well as general access to and use of the Campus. Failure to provide this information will result in access being denied to the VA IT Campus. PII will not be disseminated, shared, or used for training purposes. Authorized technical staff of ITWD will be the only users with access to PII in case of request by any individual user if needed. Some technical data (IP address, network connection speed, etc.) is also being gathered for purposes of technical support.

**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.*

Individuals have the right to decline to provide any information. However, failure to do so will result in no access to the VA IT Virtual Campus.

**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.*

No. Information is used for the sole purpose of providing TMS Credit. There are no other uses needing consent.

**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.*

**Privacy Risk:** Individuals are informed they information they input is PII and required to verify credit. A potential risk would be if an individual did not read the notice on the registration page and was unaware of the purpose of collecting their data.

**Mitigation:** The information is necessary for the application to perform its designated role. If information is not collected, the individual would not receive credit for courses taken and may not use the web application. Individuals are notified of the collection of information per the Privacy Act of 1974.

## 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.***

VA IT Virtual Campus users can access the information they provided upon registration by going into "My Profile" in the application.

*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)?*

VA IT Virtual Campus is not exempt from access provisions of the Privacy Act.

*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?*

VA IT Virtual Campus users can access the information they provided upon registration by going into "My Profile" in the application.

**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.*

VA IT Virtual Campus users can correct the information that they provided upon registration by going into "My Profile" in the application. In addition, users can contact the help desk to have a technician manually change the information.

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

*How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that*

*even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.*

Information about data correction can be found in the online help section. In addition, users can contact the help desk with any application/data related questions.

**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.*

Information about data correction can be found in the online help section. In addition, users can contact the help desk with any application/data related questions.

**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.*

**Privacy Risk:** Individual's name and TMS ID are used in the VA IT Virtual Campus web application. A potential risk would be user wouldn't know how to correct invalid information that has been entered.

**Mitigation:** At time of registration, individuals are notified their information will be used to provide credit in TMS for courses taken via a notification message on the registration page. Individuals are informed information is recorded only for the purpose of providing credit for training taken.

## 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?*

Users who have a VA PIV card are automatically registered when accessing VA IT Campus using SSOe. Users who do not have a VA PIV card can self-register using their VA email address.

Users needing to self-register should complete the required fields and click Register to submit the registration for an account or click, Cancel to terminate the registration process. The following is the account activation process which involves an email confirmed flag as well as an active flag on the account:

The Email Confirmation is sent with a link, the link must be clicked by the user and the flag Email Confirmed is set to true.

The Flag Active is set either automatically, when the primary email address is found in the TMS table, or manually by the Helpdesk.

When both flags are true, a Welcome email is sent to the Primary Email address, and the user can now log in to the website.

The User will receive an Email Confirmation email to the Primary Email address, if the primary email address matches what is in the TMS lookup table. The account will only be auto activated if the primary email is found.

The Help Desk will receive a notice to review the account if the primary email is not found, but the secondary email address is found in the TMS lookup table. Since the secondary email address is not directly tied to the user account, only the primary email address receives notifications and is used as the user account ID within the application. Only the Primary email will get an Email Confirmation message.

The Help Desk will receive a notice to review account if the primary & secondary email addresses are not found, but first name & last name combination is found in the TMS lookup table. The Primary email will get an Email Confirmation message.

If the account does not have either a primary or secondary email address in the TMS lookup table, and the first name & last name combination is not flagged for review, then the user will get a rejection email. They will not get an email confirmation.

If the user asks for a review of the rejected account, the Help Desk can send an email confirmation manually to the Primary Email address and manually set Active to true.

*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?*

If an event is marked public, outside agencies can be given read access to view the material once proper approvals are given.

*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.*

All users are given read access upon access being granted to the system. For support personnel needing to maintain the system, additional permissions can be granted upon proper approval and the completion of associated role-based training.

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

*If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

VA contractors have access to the system as long as they VA.GOV email addresses. If not, then proof that access is needed must be provided by the contractor.
VA contractors supporting the system have access to the system to provide system technical support. Prior to being granted this access, the contractor must complete associated Role-Based and Rules of Behavior training. This training is required and updated on an annual basis.

**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.*

Individuals are required to take privacy and security training at time of VA employment and yearly thereafter.

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

*8.4a If Yes, provide:*

1. *The Security Plan Status:* Completed
2. *The System Security Plan Status Date:* 3/16/2023
3. *The Authorization Status:* ATO
4. *The Authorization Date:* 12/19/2023
5. *The Authorization Termination Date:* 6/16/2024
6. *The Risk Review Completion Date:* 11/29/2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Low

*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?**
*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)*

Yes, we used the Amazon Web Services. Its authorization is FedRAMP approved.

**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.*

Contract for Amazon Web Services is provided by VAEC of the VA. Please contact the VAECSO office for specific contract information.

**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.*

Not Applicable

**9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?**

*What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

No data is held by the cloud provider for the VA IT Virtual Campus system.

**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).*

Not Applicable

## 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 |

| ID | Privacy Controls |
|---|---|
| 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** |
| 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.**

TONYA FACEMIRE

Digitally signed by TONYA FACEMIRE
Date: 2024.02.28 09:04:41 -05'00'

**Privacy Officer, Tonya Facemire**

COLLIN ROBERTS

Digitally signed by COLLIN ROBERTS
Date: 2024.02.28 07:19:20 -06'00'

**Information System Security Officer, Collin Roberts**

DANIEL JONES

Digitally signed by DANIEL JONES
Date: 2024.02.28 07:39:17 -05'00'

**Information System Owner, Daniel Jones**

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; screen shot of a website collection privacy notice).

www.vaitcampus.com

## HELPFUL LINKS:

**General Records Schedule**
https://www.archives.gov/records-mgmt/grs.html

**National Archives (Federal Records Management):**
https://www.archives.gov/records-mgmt/grs

**VA Publications:**
https://www.va.gov/vapubs/

**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