Privacy Impact Assessment for the VA IT System called:

Federal Immersive Learning Management System -Enterprise

Veterans Health Administration

SimLEARN National SimVET Center

eMASS ID #: 2541

Date PIA submitted for review:

10/31/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Phillip Cauthers	Phillip.Cauthers@va.gov	503-721-1037
Information System Security Officer (ISSO)	Martin DeLeo	martin.deleo@va.gov	202-299-6495
Information System Owner	Joseph Still	joseph.still@va.gov	717-480-7856

Abstract

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

Federal Immersive Learning Management System – Enterprise (Fed ILMS) allows for real-time collaboration, creation, and dissemination of simulation training content, scenarios, and simulation best practices. This ILMS will enable the delivery of high value care through better adoption of clinical simulation and all modalities training capabilities in the VHA.

The platform offers a comprehensive and flexible training experience, catering to both VA and non-VA users. It provides a diverse range of learning modalities, including eLearning courses, live and on-demand webinars, immersive 3D simulations, and other innovative formats. The progress and outcomes of each user's training journey are meticulously tracked, with detailed reports accessible to administrators. Additionally, users have the convenience of viewing their personal training transcripts and understanding the completion criteria for each course they enroll in.

Overview

The overview is the most important section of the Privacy Impact Assessment (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 business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?

The Federal Immersive Learning Management System -Enterprise (FED ILMS) directly supports the VHA's mission of delivering high-quality healthcare by enhancing clinical simulation training capabilities. The ILMS facilitates real-time collaboration, creation, and dissemination of simulation training content, scenarios, and best practices, enabling VHA staff to acquire and refine essential skills in a safe, controlled environment. This translates to improved patient care and outcomes across the VHA healthcare system.

B. Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.

The Federal Immersive Learning Management System -Enterprise (FED ILMS) is Software as a Service (SaaS) that will be controlled by the SimLEARN National SimVET Center program office due to their VA Partnership.

2. Information Collection and Sharing

C. Indicate the expected number of individuals whose information is stored in the system and include a brief description of the typical client or affected individual?

The typical client or affected individual may vary based on the information that is being

used in the system. The primary users are VA employees; therefore, they will be the most affected users. There are approximately 9002 to 10,000 users. The Federal Immersive Learning Management System -Enterprise (FED ILMS) is a privacy sensitive system that collects, maintains, and/or processes Personally Identifiable Information on Veterans and/or dependents, VA employees, members of the public, clinical trainees.

Check if Applicable	Demographic of individuals
☒	Veterans or Dependents
☒	VA Employees
☒	Clinical Trainees
☐	VA Contractors
☒	Members of the Public/Individuals
☐	Volunteers

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

Information is to increase the competency of trainees through simulation and other forms of e-learning. Data is used to show use of the system and allow users to create accounts.

E. What information sharing is conducted by the IT system? A general description of the modules and components, where relevant, and their functions.

The IT system shares information with the organization's Active Directory for user authentication and authorization purposes. It also shares summary reporting data with a designated data analytics system. The system has modules/subsystems dedicated to data collection, data processing and analysis, secure data storage, and report generation.

F. Are the modules/subsystems only applicable if information is shared?

No, the modules/subsystems within the Fed ILMS are not solely applicable if information is shared. They serve broader purposes in support of the system's core functionalities, even when information sharing is not involved.

G. Is the system operated in more than one site to include primary and secondary 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?

This system is not operated in more than one site.

3. Legal Authority and System of Record Notices (SORN)

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

OPM GOVT-1, "General Personnel Records" for title 5 employees, https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-1-general-personnel-records.pdf. Authority for maintenance of the system:5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 121.

76VA05 - "General Personnel Records (Title 38) – VA", https://www.govinfo.gov/content/pkg/FR-2000-07-20/pdf/00-18287.pdf. Authority for maintenance of the system: 38 U.S.C. 501(a), 7304, 7406(c)(1), and 7802.

An additional SORN is being created that will apply to the non-employee system user information that will be stored by the individual's identifier.

I. What is the SORN?

OPM GOVT-1, "General Personnel Records" for title 5 employees,
76VA05 - "General Personnel Records (Title 38) – VA",
A SORN is being created that will apply to the non-employee system user information that will be stored by the individual's identifier.

I. SORN revisions/modification

An updated SORN is currently being drafted.

J. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval.

Yes.

4. System Changes

K. Will the business processes change due to the information collection and sharing?

☐ *Yes*
☒ *No*

L. Will the technology changes impact information collection and sharing?

☐ *Yes*
☒ *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 Information 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
- ☐ **Full** Social Security Number
- ☐ **Partial** 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/Sex
- ☐ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☐ Date of Death

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

☒ Business Email Address
☐ Electronic Data Interchange Personal Identifier (EDIPI)
☒ Other Data Elements (list below)

Other PII/PHI data elements: User ID, Veteran's Integrated Service Network (VISN), Biometrics (voice and video recording), User Chat Messaging

1.2 List 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?

The system collects name and email directly from the individual during the registration process. Users are required to provide these basic details to create an account and access the system's features. We do not collect information from commercial data aggregators or other third-party sources.

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 system does not currently collect or process PII from sources other than the individuals themselves.

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

The system generates course completion scores for users.

1.3 Methods of information collection
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?

The system collects, stores, and transmits information in identifiable form using the following technologies:

Collection:

Web forms with input validation for direct user data entry. – Transmitted via secure socket layer over HTTPS.

Storage:
Encrypted relational database (e.g., Azure SQL) for PII storage using transparent Data Encryption (TDE) on the databases.

Transmission:
HTTPS for all user interactions with the system's web interface.

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?

Information is not collected on a form.

1.4 Information checks for accuracy, and how often will it be checked.

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

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

The system does not ingest information from other systems. This is the user's responsibility when populating the system with their information and it is their responsibility to update the system to be accurate.

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 system does not check for accuracy by accessing a commercial aggregator of information.

1.5 Identify the specific legal authorities, arrangements, and agreements that 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

OPM GOVT-1, "General Personnel Records" for title 5 employees,

https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-1-general-personnel-records.pdf. Authority for maintenance of the system:5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 121.

76VA05 - "General Personnel Records (Title 38) – VA", https://www.govinfo.gov/content/pkg/FR-2000-07-20/pdf/00-18287.pdf. Authority for maintenance of the system: 38 U.S.C. 501(a), 7304, 7406(c)(1), and 7802.

An additional SORN is being created that will apply to the non-employee system user information that will be stored by the individual's identifier.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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: The collection ties with the purpose of the underlying mission of the organization and its enabling authority.

Principle of Minimization: The information is directly relevant and necessary to accomplish the specific purposes of the program.

Principle of Individual Participation: The program, to the extent possible and practical, collects information directly from the individual.

Principle of Data Quality and Integrity: VA policies and procedures must ensure that personally identifiable information is accurate, complete, and current.
This 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:

- PII Sensitivity: The FED ILMS collects a range of PII, including name, email addresses (personal and business), user ID, VISN, Biometrics (voice and video recording), user chat messaging. This diverse data collection significantly increases privacy risks, as the potential for unauthorized access, disclosure, or misuse could lead to identity theft, discrimination, reputational harm, or even safety concerns.
- Identifiability: The combination of various data elements, particularly those related to user activity and performance, significantly increases the risk of re-identification. This could expose individuals to targeted attacks, profiling, or unwanted disclosures.

- Sensitive Content: Voice, video, and chat communication may contain highly personal or sensitive information, further amplifying privacy risks if compromise.

Mitigation:

- Minimization: The FED ILMS collects only the minimum necessary PII required to fulfill its educational mission, aligning with the principles of Privacy by Design.
- Encryption: PII is encrypted both at rest (using AES-256 encryption in Azure SQL Database and Azure Blob Storage) and in transit (using HTTPS with TLS 1.2 or higher).
- Access Controls: Strict role-based access controls (RBAC) are implemented, ensuring that only authorized personnel can access specific data based on their roles and responsibilities within the system.
- Purpose Limitation: Technical controls, including database views and stored procedures, are implemented to restrict data access and usage to only what is necessary for the intended educational purposes.
- Data Retention: A data retention policy is in place to ensure that PII is not retained longer than necessary for legitimate business or educational purposes. Data is securely purged or anonymized after the retention period.
- Privacy Notices: Clear and comprehensive privacy notices are provided to users upon registration and are readily accessible within the system. These notices inform users of data collection practices, purposes, and their rights under applicable privacy laws.
- Audit Logs: The FED ILMS maintains detailed audit logs of all system activity, including data access, modifications, and potential security events. These logs are regularly reviewed to detect and investigate any unauthorized or suspicious activity.
- Regular Security Assessments: The FED ILMS undergoes regular security assessments, including vulnerability scans and penetration testing, to identify and address potential security weaknesses that could expose PII.

By incorporating these mitigation measures, the FED ILMS demonstrates a strong commitment to protecting user privacy and adhering to best practices in data security and privacy.

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	• File Identification purposes	• Not used

Personal Email Address	• User authentication & login. • Account management notifications. • User-to-user communication.	• Account recovery communications. • Limited marketing or informational emails (if consent is obtained).
Business Email Address	• User authentication & login. • Account management notifications. • User-to-user communication.	• Account recovery communications. • Limited marketing or informational emails (if consent is obtained).
User ID	• User authentication & login. • Account management notifications. • User-to-user communication.	• Account recovery communications. • Limited marketing or informational emails (if consent is obtained).
VISN	• Track User Learning Data	• NA
Biometrics (voice and video recording)	• Participate in meetings/events with other system users. • Optional Recording for archiving and learning data collection.	• Participate in meetings/events and chats with other system users. • NA for Veterans and Academia. • Optional Recording of Other Govt. Agencies for archiving and learning data collection
User chat messaging	• Participate in meetings/events and chats with other system users. • Optional Recording for archiving and learning data collection.	• Participate in meetings/events and chats with other system users. • NA for Veterans and Academia. • Optional Recording of Other Govt. Agencies for archiving and learning data collection

2.2 Describe the types of tools 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?

Reporting: The system generates usage reports that summarize user activity, course completion rates, and overall system engagement metrics. While these reports aggregate data, they do not reveal individual PII. These reports are further secured to only the administrative users which have been granted access to this information within their sphere of reporting influence.

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 FED ILMS generates usage reports that summarize user activity, course completion rates, and overall system engagement. These reports primarily aggregate data and do not directly create new PII about individuals. However, in some instances, authorized administrators may generate individual user reports for specific purposes, such as assessing progress or identifying areas for personalized support.

- Individual Reports: These reports may indirectly reveal previously unutilized information about an individual's learning patterns, strengths, and areas needing improvement.
    - Storage: Individual user reports are stored securely within the Azure SQL database, utilizing encryption at rest to protect the data.
    - Impact on Users: Individual reports may be used to inform performance reviews or identify areas for additional training. However, they are not the sole basis for employment decisions.
    - Usage: These reports are accessed and utilized by authorized supervisors and trainers to tailor training programs, provide personalized feedback, and support individual learning goals. The reports may also be shared with the individual user to foster self-awareness and guide their professional development.

- Aggregated Reports: These reports do not identify individual users and are used to assess overall training effectiveness, identify trends, and inform program-level improvements.
    - Storage: Aggregated reports are stored securely in Azure Blob Storage with encryption at rest.
    - Access: Aggregated reports are accessible to authorized administrators and program managers responsible for evaluating training programs and making data-driven decisions.

2.3 How the information in the system is 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?

All data at rest is encrypted using FIPS validated AES 256-bit encryption via Azure storage encryption. Data stored in the Azure SQL Databases additionally have transparent data encryption enabled using Microsoft Managed Keys.

All data in transit is encrypted using TLS 1.2 and all connections with Azure Services (e.g., Azure SQL, Blob storage, Azure Cache for redis) are accomplished via Private Endpoints to eliminate any possibility of MITM attacks.

All portions of the application are only available to authenticated users of the application and all traffic to the application traverses a DMZ with WAF policies in place to protect the back end.

All CSP users utilize hardware token MFA for all access to the system.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? (refer to PTA question 3.8).

SSNs are not collected, processed, or retained.

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

All data at rest is encrypted using FIPS validated AES 256 bit encryption via Azure storage encryption. Data stored in the Azure SQL Databases additionally have transparent data encryption enabled using Microsoft Managed Keys.

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?

Access to PII is granted by the VA based on their internal policies and procedures and a valid need to know. CSP users are granted access leveraging RBAC, these users are all approved by the Change control board and the deployment administrator/ISSO.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented? How are the documented, i.e. Policy, SOP, other. And where is this documentation located?

Criteria, procedures, controls, and responsibilities are documented in the Fed ILMS Appendix C ISPP document for CSP users. The VA SOP will document these requirements for the VA personnel.

2.4c Does access require manager approval?

Yes, CSP users are granted access leveraging RBAC, these users are all approved by the Change control board and the deployment administrator/ISSO.

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

Yes, leveraging Azure Monitoring, Microsoft Defender for Cloud, Azure Sentinel and the applications robust auditing and logging capabilities. The VA is responsible for auditing authentication checks for users authenticated by their Active Directory or IDP (Identity Provider).

2.4e Who is responsible for assuring safeguards for the PII as identified in eMASS?

Creative Veteran Productions (CVP) is responsible for assuring the safeguards are in place, having this audited by a 3PAO ~~Third Party Assessment Organization~~ on an annual basis. The VA is responsible for verifying the results of the assessment are within the VAs risk tolerance and issuing an ATO for the system.

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

The Fed ILMS retains the following information collected from users, as outlined in question 1.1:

- **Name:** User's full name is retained for identification and record-keeping purposes.
- **Personal Email:** Retained for communication and account recovery purposes.
- **Business Email:** Retained for communication and account recovery purposes.

- **User ID:** A unique identifier assigned to each user, retained for system functionality and data management.
- **Veteran's Integrated Service Network (VISN):** Retained for reporting and analysis purposes, allowing the VA to track usage and engagement across different regions.
- **Biometrics (voice and video recording):** If biometrics are used for authentication, they are securely stored and processed in accordance with relevant privacy and security standards.
- **User Chat Messaging:** Chat logs may be retained for a limited time for quality assurance, monitoring, or support purposes.

Data retention policies:
The retention of this information is governed by the Fed ILMS's data retention policies, which are aligned with:

- **DM-1, Minimization of Personally Identifiable Information:** We strive to collect and retain only the minimum necessary PII to fulfill the system's purpose.
- **DM-2, Data Retention and Disposal:** We have established clear procedures for data retention and disposal, ensuring compliance with relevant regulations and VA policies.

Additional Considerations:

- **Data Security:** All retained information is protected with appropriate security controls, including encryption and access restrictions.
- **User Rights:** Users have the right to access, correct, or request deletion of their personal information, subject to any legal or regulatory obligations for data retention.

.

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 https://www.archives.gov/records-mgmt/grs? This question is related to privacy control DM-2, Data Retention and Disposal.*

Records in this system are retained and disposed of in accordance with the schedule approved by the Archivist of the United States, Records Control Schedule (RCS) 10-1,, item 1100.40B, all VA employees and clinical trainees' records will be maintained for 7 years according to the RCS 1100.40B. Federal Immersive Learning Management records pertaining to Veterans, Dependents and members of the public records will be unscheduled and maintained indefinably. Any data destruction done on behalf of VA by a Contractor/Subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, Records and Information Management and its Handbook 6300.1 Records Management Procedures, applicable VA Records Control Schedules, and VA Handbook 6500.1, Electronic Media Sanitization. Self-certification by the Contractor that the

data destruction requirements above have been met must be sent to the VA CO within 30 days of termination of the contract.

3.3 The retention schedule 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. Please work with the system 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. Records in this system are retained and disposed of in accordance with the schedule approved by the Archivist of the United States, Records Control Schedule (RCS) 10-1, item 1100.40B, all VA employees and clinical trainees' records will be maintained for 7 years according to the RCS 1100.40B. Federal Immersive Learning Management records pertaining to Veterans, Dependents and members of the public records will be unscheduled and maintained indefinably.

Non-VA individual's information collected by the system will be maintained indefinitely until a SORN applicable to that information is published and a records control schedule is identified for it.

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

Records in this system are retained and disposed of in accordance with Records Control Schedule (RCS) 10-1, item 1100.40B, with disposition authority N1-015-11-4, item 2.

Non-VA individual's information collected by the system will be maintained indefinitely until a SORN applicable to that information is published and a records control schedule is identified for it.

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.

When a resource such as a VM or PaaS services is no longer needed and the agency's data is returned to them following a contract termination, Project Hosts on CVP's behalf deletes the resource following the instructions provided by Microsoft to ensure the data and disks are appropriately deleted and sanitized as detailed in the FED ILMS SSP Appendix P SCRM.

The methods in which they are deleted after selecting the appropriate option in the Azure portal is inherited from Microsoft Azure Government (F1603087869) through its managed service provider Project Hosts who deploys all of the services on CVP's behalf within the

Microsoft Azure Government boundary and has the appropriate agreements in place with Microsoft.

By default, data is retained in the Fed ILMS database for the lifetime of the contract.

Retention Schedule: Data is retained for 7 years. Any data destruction done on behalf of VA by a Contractor/Subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, Records and Information Management and its Handbook 6300.1 Records Management Procedures, applicable VA Records Control Schedules, and VA Handbook 6500.1, Electronic Media Sanitization. Self-certification by the Contractor that the data destruction requirements above have been met must be sent to the VA CO within 30 days of termination of the contract.

Disposal Triggers: "Upon reaching the designated retention period, the system automatically flags the data for disposal or transfer, depending on its nature."

Disposal Methods:

Electronic Data: "Electronic data is securely overwritten using industry-standard data sanitization methods before secure deletion." (Specify the standard, e.g., NIST SP 800-88)

On-Site Shredding: N/A. System does not retain paper records.

VA Disposition Schedule: Ensure your retention periods and disposal methods align with the relevant VA Disposition Schedule, which outlines record series retention requirements. User access is periodically reviewed to ensure it remains aligned with their current roles and responsibilities. Privileged accounts are reviewed at least quarterly and user accounts at least every 6 months for compliance with account management requirements within the Federal Immersive Learning Management System -Enterprise application. Course training information will sunset based on life cycle of the course and follow NARA guidelines after sunset.

NARA Transfer: For records with historical value identified for permanent retention, the system will generate a transfer request to the National Archives and Records Administration (NARA) in accordance with established procedures.

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.

This information is never used for research, testing nor training.

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 Privacy Officer (PO) 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: The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.

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

Follow the format below:

Privacy Risk: There is a risk that the information maintained by the Fed ILMS system will be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation:

Part a:

CVP has developed and documented a security and privacy architecture for the system that describes the requirements and approach to be taken for protecting the Confidentiality, Integrity and availability of CVP information as well as processing personally identifiable information to minimize privacy risk to individuals. This security and privacy architecture are integrated into and support the enterprise architecture as well as assumptions, and dependencies on external systems and services. This is documented in more detail in the FED ILMS system security plan in sections 7-10.

Records in this system are retained and disposed of in accordance with the schedule approved by the Archivist of the United States, Records Control Schedule (RCS) 10-1, item 1100.40B, all VA employees and clinical trainees' records will be maintained for 7 years according to the RCS 1100.40B. Federal Immersive Learning Management records pertaining to Veterans, Dependents and members of the public records will be unscheduled and maintained indefinably . Any data destruction done on behalf of VA by a Contractor/Subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, Records and Information Management and its Handbook 6300.1 Records Management Procedures, applicable VA Records Control Schedules, and VA Handbook 6500.1, Electronic Media Sanitization. Self-certification by the Contractor that the data destruction requirements above have been met must be sent to the VA CO within 30 days of termination of the contract.

When a resource such as a VM or PaaS services is no longer needed and the agency's data is returned to them following a contract termination, Project Hosts on CVP's behalf deletes the resource following the instructions provided by Microsoft to ensure the data and disks are appropriately deleted and sanitized as detailed in the FED ILMS SSP Appendix P SCRM.

The methods in which they are deleted after selecting the appropriate option in the Azure portal is inherited from Microsoft Azure Government (F1603087869) through its managed service provider Project Hosts who deploys all of the services on CVP's behalf within the Microsoft Azure Government boundary and has the appropriate agreements in place with Microsoft.

These protections are implemented through a security architecture consisting of layered security, access control based upon a least privilege model, and continuous monitoring to verify consistent application of security controls. The FED ILMS system has separate dedicated subnets for a test deployment, and a production deployment. Application updates are tested and scanned in the test deployment before being implemented in production deployments.

Part b:

CVP ISSO and Project Hosts security team reviews and updates the architecture at least annually or when a significant change occurs to reflect changes in the enterprise architecture and reflects these changes in security and privacy plans, CONOPS documentation, organizational procedures, procurements and acquisitions and ensures that appropriate criticality/security impact analysis are completed for each change.

Part c:

CVP ISSO and Project Hosts security team reviews and updates the architecture at least annually or when a significant change occurs to reflect changes in the enterprise architecture and reflects these changes in security and privacy plans, CONOPS documentation, organizational procedures, procurements and acquisitions and ensures that appropriate criticality/ security impact analysis are completed for each change.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

PII Mapping of Components

4.1a **Federal Immersive Learning Management System (FED ILMS) -e** consists of **2** key components (servers/databases/instances/applications/software/application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **Federal Immersive Learning Management System (FED ILMS) -e** 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 3.9a in the PTA should be used to answer this question.

Internal Components Table

Component Name (Database, Instances,	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

Application, Software, Application Program Interface (API) etc.) that contains PII/PHI					
Talent Management System (TMS)	Yes	Yes	Name Personal E-mail Business E-mail User Chat Messaging User ID	System operation.	HTTPS, Encryption at rest

4.1b List internal organizations information is shared/received/transmitted, the information shared/received/transmitted, and the purpose, and how the information is transmitted.

NOTE: Question 3.9b (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

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
Talent Management System (TMS)	Users are required to provide these basic details to create an account and access the system's features.	• Name • Personal E-mail • Business E-mail • User Chat Messaging • User ID	Hyper Text Transfer Protocol (HTTP) with Secure Sockets Layer (SSL) at the point of collection and storing of the most sensitive data points in an encrypted data table that cannot be accessed via the application interface. Employee profiles are either directly sourced from VA's HR system of record or manually entered through a web-interface inside the VA firewall. Data is communicated to TMS 2.0 via Secure File Transfer Protocol (SFTP) and then stored in the encrypted data table that cannot be accessed via the

IT system and/or Program office. Information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List PII/PHI data elements shared/received/transmitted.*	*Describe the method of transmittal*
			application interface. Least privilege principle is applied when granting administrative access to TMS 2.0 where data other than SSN and DOB can be viewed via the application interface.

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the VA network 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 in this section.).

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

Follow the format below:

Privacy Risk:

- PII Sensitivity: The system collects sensitive PII, including name and email address, this creates privacy risks related to unauthorized access, disclosure, or misuse.
- Identifiability: Collected PII elements could potentially be combined to re-identify individuals, exposing them to privacy risks.

Mitigation: FED ILMS implement RBAC, encryption of data in transit and rest and strict access controls along with robust auditing capabilities and a thorough security awareness training program.

- Minimization: The system adheres to the principle of data minimization, collecting only the PII strictly necessary for its core functions.
- Encryption & Access Controls: PII is protected with strong encryption at rest and in transit. Role-based access controls (RBAC) enforce the principle of least privilege.
- Purpose Limitation: Technical and procedural safeguards are in place to prevent the use of PII for purposes beyond the explicitly stated mission of the system.
- Transparency: Clear privacy notices inform individuals about information collection, use, and their rights regarding their data.

- Auditing & Logging: Regular audits and detailed logging mechanisms help detect and investigate potential privacy breaches.

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 List the external organizations (outside VA) that information shared/received. and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.

The sharing of information outside the agency must be compatible with the original collection. The sharing must be covered by an appropriate routine use in a SORN. If not covered, 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 IT System or External Program Office information is shared/received with	***List the purpose of information being shared / received / transmitted***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)***	***List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be***	***List the method of transmission and the measures in place to secure data***

			more than one)	
Twilio	To enable voice communication between the app and Twilio. Non-identifying user information or metadata (e.g., call duration, timestamps) for operational purposes. No phone numbers are collected from users. Communication is strictly between the Fed ILMS and Twilio.	Non-identifying user information or metadata may be transmitted via the aforementioned connections. The purpose is to enable voice communication between the app and Twilio. No Phone numbers are collected form users. The connections that happen are strictly between the app and Twilio.	Twilio : MSA, SLA, DPA (or Terms of Service, or Explicit User Consent), ISA	HTTPS, TLS 1.2, for Twilio the API is authenticated using Twilio Client Capability tokens.
Digital Samba	For the purposes of providing live webinar sessions and other essential platform functionality. Broadcasting user video and audio. Chat messaging and content sharing. Data Shared/Received : Audio and video data for real-time communication. Chat messages and shared content.	To provide platform functionality such as broadcasting user video and audio to other users previously authenticated through the system, chat messaging and content sharing amongst users as well for user identification on the platforms. This information can be non-identifiable information such as a chosen username.	Samba: DS Customer Agreement, SLP, AUP, ISA	HTTPs TLS 1.2 for Digital Samba the API is authenticated using JWT tokens and bearer tokens, data is purged automaticall y after 90 days but can also be purged on demand.

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

Follow the format below:

Privacy Risk:

- PII Sensitivity: The system collects sensitive PII, including name and email address, this creates privacy risks related to unauthorized access, disclosure, or misuse.
- Identifiability: Collected PII elements could potentially be combined to re-identify individuals, exposing them to privacy risks.

Mitigation:

- Minimization: The system adheres to the principle of data minimization, collecting only the PII strictly necessary for its core functions.
- Encryption & Access Controls: PII is protected with strong encryption at rest and in transit. Role-based access controls (RBAC) enforce the principle of least privilege.
- Purpose Limitation: Technical and procedural safeguards are in place to prevent the use of PII for purposes beyond the explicitly stated mission of the system.
- Transparency: Clear privacy notices inform individuals about information collection, use, and their rights regarding their data.
- Auditing & Logging: Regular audits and detailed logging mechanisms help detect and investigate potential privacy breaches.

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 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms, notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.

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 Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.

See image in Appendix. Text contains the following: By logging in or registering for an account, you acknowledge that the VA will collect and store certain personal information, including your name, email address, and any other information you provide in your profile. This information will be used to manage your access to the Fed ILMS, track your learning progress, and provide you with relevant training and development opportunities.

The SORNS OPM GOVT-1, "General Personnel Records" for title 5 employees, https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-1-general-personnel-records.pdf and 76VA05 - "General Personnel Records (Title 38) – VA", https://www.govinfo.gov/content/pkg/FR-2000-07-20/pdf/00-18287.pdf also provide notice to employees and trainees about information that will be collected.

This Privacy Impact Assessment (PIA) also serves as notice 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.

A notice was provided.

6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.

The privacy notice displayed on the Fed ILMS login/registration page adequately informs users that their information is being collected and used appropriately. It achieves this through:

- Explicit Statement of Collection: The notice clearly states that the VA will "collect and store certain personal information," which includes, but is not limited to, the user's name and email address.
- Purpose Limitation: The notice specifies the purposes for which the information will be used: "to manage your access to the Fed ILMS, track your learning progress, and provide you with relevant training and development opportunities." This assures users that their data will be used for legitimate and intended purposes.
- Link to Full Privacy Policy: The notice provides a direct link to the VA's comprehensive privacy policy (https://www.va.gov/privacy-policy) for users who wish to learn more about the VA's data protection practices.

Additionally, the notice is prominently displayed on the login/registration page, ensuring users see it before submitting any personal information. The notice uses clear and concise language, avoiding technical jargon, to ensure it is easily understandable for all users.

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 do have the opportunity and right to decline to provide certain information to the Fed ILMS. However, some information is essential for account creation and access to the system. Declining to provide mandatory information may result in the inability to create an account or access certain features of the Fed ILMS.

- Mandatory Information: Information required for account creation and basic functionality (name, email address) is mandatory. Declining to provide this information will result in denial of service.
- Optional Information: Users may choose to provide additional information in their profiles to enhance their experience. Declining to provide this optional information will not result in any penalty or denial of service.

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.

The Fed ILMS requires certain information for user authentication, personalization, and effective course delivery. Individuals do not have the option to selectively consent to the specific uses of the data elements collected; therefore, the only alternative for those who do not wish to share their information is to refrain from using the system. While some fields within the application, such as Title, Phone Number, and Profile Picture, are optional, providing this information is not a prerequisite for accessing the system's core functionalities. Any uses outside that defined scope would require additional notice and consent unless other legal authority is identified.

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

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 Privacy Officer (PO) to complete all Privacy Risk questions inside the document this section).

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

<u>Principle of Transparency:</u> This is referring to sufficient notice provided to the individual.

<u>Principle of Use Limitation:</u> The information used only for the purpose for which notice was provided either directly to the individual or through a public notice. The procedures in place must 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 individuals may not receive adequate notice that their information is being collected, maintained, or disclosed by Fed ILMS before they provide the information to the VA. This lack of sufficient notice could lead to:

Misunderstanding and Mistrust: Users may feel their privacy has been violated if they are unaware of the data collection practices.
Lack of Informed Consent: Users may not be able to provide meaningful consent for the collection and use of their data if they are not fully informed.
Potential Harm: In some cases, the lack of notice could lead to potential harm, such as identity theft or discrimination, if sensitive information is collected or shared without the user's knowledge.

Mitigation:

- Targeted Notices:
    - Employees and non-VA individuals are provided with a direct notice regarding the collection of their information, as detailed in section 6.1a and Appendix A of this PIA.
    - All other users are provided with a privacy notice at the point of information collection, such as during login/registration or within specific courses and modules. These notices inform users about the data collection practices relevant to their interactions with the system.

- Publicly Available Documentation: Additional mitigation is provided by making the System of Records Notices (SORNs) and this Privacy Impact Assessment (PIA) available for public review. This promotes transparency and allows individuals to understand how their information is being collected, used, and protected.

- Use Limitation (UL-1): Information collected by Fed ILMS is used only for the purposes stated in the privacy notices. Technical and procedural safeguards are in place to prevent unauthorized access, use, or disclosure of data.

- Data Minimization (DM-1): The system adheres to the principle of data minimization, collecting only the information necessary for its core functions, further reducing the risk of unintended data collection or use.

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 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 VA Public Access Link-Home (efoia-host.com) to obtain information about FOIA points of contact and information about agency FOIA processes.***

All users must enter authentication information to gain access to their information. Individuals may personally ensure that all of their user profile information is accurate and can directly make changes to portions of this information. Users can view, edit, and update their personal information within their user profile settings. Individuals can submit a formal FOIA/Privacy Act request to the VA to access their information. The VA has designated FOIA points of contact and processes to handle such requests. For more information, please refer to the VA FOIA Web page at VA Public Access Link-Home https://vapal.efoia-host.com/. See image in Appendix.

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)?

The system is not exempt from the Privacy Act. SORNs have been identified for the VA employee information and a SORN is being created for the non-VA individual's information.

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?

The system is Privacy Act system.

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.

The user can correct the information themselves within the application and/or notify the system administrator.

Users can correct most inaccurate or erroneous information themselves within the Fed ILMS application by following these steps:

1. Log in to the Fed ILMS.

2. Click on the profile button on the bottom navigation bar, which brings up the profile component.
3. Click on the “Edit Information” button within the profile window.
4. Update the relevant information in their profile, such as their name, email address, job title, or contact details.
5. Click the Save button to save the changes.

Contacting Support

If users encounter any difficulties correcting their information or need to update data that is not editable within their profile, they can contact the Fed ILMS Help Desk for assistance. The Help Desk can be reached through phone, email, and online form.

Additional Considerations

- Verification: The Help Desk may require verification of the user's identity before making any changes to their information.
- Data Sensitivity: For certain sensitive data elements, there may be specific procedures or restrictions on correction to ensure data integrity and compliance with regulations. Accessibility: Ensure that the profile editing process is accessible to users with disabilities, including those using assistive technologies.

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.

Users can update their information by logging into the system, navigating to their profile page, and clicking the "Edit Information/profile" button. Editable fields are clearly identified, and instructions for making changes are provided.

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.

Users can update their information by logging into the system, navigating to their profile page, and clicking the "Edit Information/profile" button. Editable fields are clearly identified, and instructions for making changes are provided.

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 Privacy Officer (PO) to complete all Privacy Risk questions in this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: The individual must be provided with the ability to find out whether a project maintains a record relating to them.

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

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

Follow the format below:

Privacy Risk:
There is a risk that Fed ILMS users may not be aware of the procedures for accessing, correcting, or updating their personal information within the system. This lack of awareness could lead to:

- Inaccurate or Outdated Data: If users don't know how to update their information, the system may contain outdated or inaccurate data, which could lead to inefficiencies or miscommunications.
- Frustration and Dissatisfaction: Users may become frustrated if they are unable to easily access or correct their information.
- Privacy Concerns: Users may have concerns about the accuracy and control of their personal information if they are unaware of the mechanisms for accessing and correcting it.

Mitigation:
To mitigate this risk, Fed ILMS has implemented the following strategies:

- Clear and Accessible Instructions: Provide clear and user-friendly instructions on how to access and update personal information within the system. These instructions can be included in:
    - Help Center and FAQs: Develop dedicated help articles or FAQs that specifically address accessing and correcting user information.
    - User Guides and Tutorials: Incorporate instructions on profile management and data correction into user guides and training materials.

    - On-Screen Prompts: Provide clear on-screen prompts and guidance within the Fed ILMS interface to help users navigate their profile settings and make updates.
- Help Desk Support: Ensure that the Fed ILMS Help Desk is readily available to assist users with any questions or difficulties they encounter while accessing or correcting their information.

- Regular Communication: Periodically remind users of their rights to access and correct their information and provide links to relevant resources.

- Accessibility: Ensure that the procedures for accessing and correcting information are accessible to users with disabilities, including those using assistive technologies.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures. (Work with your ISSO to complete this section).

8.1 The procedures in place to determine which users may access the system, must be 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?

Access to PII is granted by the VA based on their internal policies and procedures and a valid need to know. Typically for other VA projects it is accomplished via a Service Now (SNOW) ticket being put in requesting access and then the VA ISSO/ISSM for the Fed ILMS system would put them in the proper AD group to access via SSO or federation. The VA Agency administrator would then provide the user with the proper roles inside of the application.

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

No other agencies have access to the Fed ILMS.

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.

Web Users:

Users can register to access the system and if required the login approvals can be controlled by the system Administrator. When fully registered a user can:

1. Access the main lobby and navigate the site using a map.
2. Use robust search functionalities to find content and events.
3. Create and edit their profiles.
4. Attend the virtual exhibit hall.
5. Navigate to and interact within the auditorium.
6. Save content as favorites and access transcripts.

CMS Users:

Access is granted granularly and can be controlled by the system Administrator. This granular access has the following sections within the CMS:

1. Dashboards:
    a. The DASHBOARD is the quick event reference page for users that have the ViewDashboard permissions. Upon selecting the Dashboard tab - the following page is displayed:
2. Events:
    a. The Events tab gives you access to creating and managing each event's details.
3. Exhibit Hall:
    a. Admin users with ViewExhibitHall privileges have access to the Exhibit Hall tab within CMS. They can adjust booths and posters.
4. Banners:
    a. Admin users with Banner privileges can have access to edit banners.
5. Reports:
    a. Admin users with CanViewReports privileges have access to the Reports drop-down list in the CMS, however, users need privileges to run the individual reports. Currently there are tenreports Registration,User Login, WBT Completion, Rating Activity, TMS Session Roster,TMS User Data, Absent Users, Live Users, Evaluations, and CME Report through the Reports tab.
6. Courses:
    a. Admin users with ViewCourse privileges have access to the CMS Courses section. The Courses section is to primarily manage the WBT's (Web Based Training) content on the FedILMS site.
7. Media:
    a. Admin users with ViewMedia privileges have access to the Media section of the CMS. The Media tab gives you access to 2 key media functions, managing the media that will be available in the FedILMS site and building the interview tree that will used in the Library's Interview Search function.
8. Email:
    a. Admin users with ViewEmailTemplate privileges have access to the Email dropdown menu which has 3 options, manage email templates, write an email using a template or not, view a log of all the emails sent by an admin from the system.
9. Users:
    a. Admin users with ViewUsers privileges can access the Users tab. By default, the user list is filtered by registered campus users that are marked Inactive and Locked Out.
10. Authors:
    a. Admin users with ViewAuthor privileges have access to the Authors in the CMS. In the Authors tab, the admin is presented with a list of authors currently available in the system.

8.2a. Will VA contractors have access to the system and the PII? Yes

8.2b. What involvement will contractors have with the design and maintenance of the system?

Contractors will not be involved with the design and maintenance of the system. These contractors would be users who are not the owners or vendor but are rather users that could need to access the system to perform their duties.

8.2c. Does the contractor have a signed confidentiality agreement?

Yes. All contractors granted access to Fed ILMS are required to sign a Non-Disclosure Agreement (NDA) before access is granted.

8.2d. Does the contractor have an implemented Business Associate Agreement for applicable PHI?

No, the contractor does not handle PHI, therefore a BAA is not required.

8.2e. Does the contractor have a signed non-Disclosure Agreement in place?

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

Yes, Contractors sign an NDA prior to accessing the Fed ILMS.

Contractor agreements are reviewed annually by the Contracting Officer's Representative (COR)

Contractors may require access to Fed ILMS to perform their duties such as e.g., "providing technical support or assisting with training development. Access is granted based on the principle of least privilege, meaning contractors are only given the minimum level of access necessary to perform their duties. Clearance is not required for the tasks performed by contractors within Fed ILMS.

User Roles and access levels:

Web Users:

Users can register to access the system and if required the login approvals can be controlled by the system Administrator. When fully registered a user can:

1. Access the main lobby and navigate the site using a map.
2. Use robust search functionalities to find content and events.
3. Create and edit their profiles.
4. Attend the virtual exhibit hall.
5. Navigate to and interact within the auditorium.
6. Save content as favorites and access transcripts.

CMS Users:

Access is granted granularly and can be controlled by the system Administrator. This granular access has the following sections within the CMS:

11. Dashboards:
    a. The DASHBOARD is the quick event reference page for users that have the ViewDashboard permissions. Upon selecting the Dashboard tab - the following page is displayed:
12. Events:

a. The Events tab gives you access to creating and managing each event's details.

13. Exhibit Hall:
    a. Admin users with ViewExhibitHall privileges have access to the Exhibit Hall tab within CMS. They can adjust booths and posters.
14. Banners:
    a. Admin users with Banner privileges can have access to edit banners.
15. Reports:
    a. Admin users with CanViewReports privileges have access to the Reports drop-down list in the CMS, however, users need privileges to run the individual reports. Currently there are tenreports Registration,User Login, WBT Completion, Rating Activity, TMS Session Roster,TMS User Data, Absent Users, Live Users, Evaluations, and CME Report through the Reports tab.
16. Courses:
    a. Admin users with ViewCourse privileges have access to the CMS Courses section. The Courses section is to primarily manage the WBT's (Web Based Training) content on the FedILMS site.
17. Media:
    a. Admin users with ViewMedia privileges have access to the Media section of the CMS. The Media tab gives you access to 2 key media functions, managing the media that will be available in the FedILMS site and building the interview tree that will used in the Library's Interview Search function.
18. Email:
    a. Admin users with ViewEmailTemplate privileges have access to the Email dropdown menu which has 3 options, manage email templates, write an email using a template or not, view a log of all the emails sent by an admin from the system.
19. Users:
    a. Admin users with ViewUsers privileges can access the Users tab. By default, the user list is filtered by registered campus users that are marked Inactive and Locked Out.
20. Authors:
    a. Admin users with ViewAuthor privileges have access to the Authors in the CMS. In the Authors tab, the admin is presented with a list of authors currently available in the system.

VA contractors may require access to PII to potentially help troubleshoot user issues, generate reports on user activity, or develop training materials that are tailored to user needs. Access to PII is strictly controlled and limited to what is necessary for contractors to fulfill their contractual obligations.

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.

All CSP users take the following training: Security and privacy awareness training, insider threat training, information spillage training, counterfeit prevention awareness training and role-based training on an annual basis.

8.4 The Authorization and Accreditation (A&A) completed for the system.

8.4a If Yes, provide:

1. *The Security Plan Status:* <<ADD ANSWER HERE>>
2. *The System Security Plan Status Date:* <<ADD ANSWER HERE>>
3. *The Authorization Status:* <<ADD ANSWER HERE>>
4. *The Authorization Date:* <<ADD ANSWER HERE>>
5. *The Authorization Termination Date:* <<ADD ANSWER HERE>>
6. *The Risk Review Completion Date:* <<ADD ANSWER HERE>>
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* <<ADD ANSWER HERE>>

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.***

VA Sponsored FedRAMP ATO process is the initial A&A process for the Federal Immersive Learning Management System (FED ILMS) SaaS application and is In Process. The following items are included in this process: Security Plan, Authorization, and Risk Review. The estimated IOC date is September 29, 2025. The system is currently classified as Moderate Impact."

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. ***(Refer to question 1.8 of the PTA)***

This system is a Software as a Service (SaaS) that uses cloud technology. There is no current agency authorization or FedRAMP Authorization for the solution, but it is currently in process of pursuing a VA-Sponsored FedRAMP Authorization. The system has a current data security categorization of Moderate from VA's Digital Transformation Center. Both a PIA and PTA have been completed and approved by the VA Privacy Office.

9.2 Does the contract with the Hosting 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 3.3.1 of the PTA)* *This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

Yes. Contract: GS-02F-0054V; Task Order: 36C10B23F0355. Section B2 Governing Rights Clause. Section B5 INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE.

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

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

No, none of this data is mapped to the VA or any other customers.

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.

Yes. Section B5 of the contract - INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE. B5 clearly demonstrate the alignment between the FedILMS service offerings and the principle of organizational accountability for data security and privacy in cloud environments. FedILMS recognizes that the VA retains ultimate responsibility for its data, and we are committed to providing the necessary security controls, compliance measures, and transparency to support the VA in fulfilling its obligations.

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).

The system does not use 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**
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.

PHILLIP CAUTHERS

Digitally signed by PHILLIP CAUTHERS
Date: 2025.02.11 09:06:08 -08'00'

Privacy Officer, Phillip Cauthers

JOHN DELEO

Digitally signed by JOHN DELEO
Date: 2025.02.11 12:52:35 -05'00'

Information System Security Officer, Martin DeLeo

JOSEPH STILL

Digitally signed by JOSEPH STILL
Date: 2025.02.11 13:05:35 -05'00'

Information System Owner, Joseph Still

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; screen shot of a website collection privacy notice).

Privacy notice at login screen referenced in section 6.1a above.

VA FOIA notice at login screen referenced in section 7.1a above.

On the login screen for FED ILMS, the following text is displayed:

> By logging in or registering for an account, you acknowledge that the VA will collect and store certain personal information, including your name, email address, and any other information you provide in our profile. This information will be used to manage your access to the Fed ILMS, track your learning progress, and provide you with relevant training and development opportunities.
>
> For more details about our privacy practices, please refer to the VA's Privacy Policy (linked) and the Veterans Affairs Freedom of Information Act (linked).

VA Privacy Policy: Privacy, Policies, And Legal Information | Veterans Affairs

VA Freedom of Information Act: https://vapal.efoia-host.com/

SORNS OPM GOVT-1, "General Personnel Records" for title 5 employees, https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-1-general-personnel-records.pdf

SORN 76VA05 - "General Personnel Records (Title 38) – VA", https://www.govinfo.gov/content/pkg/FR-2000-07-20/pdf/00-18287.pdf

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

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): IB 10-163p (va.gov)
VHA Directive 1605.04 Notice of Privacy Practices