Date of Approval: **August 25, 2023**

PIA ID Number: **8174**

SYSTEM DESCRIPTION

Enter the full name and acronym for the system, project, application and/or database.

Integrated Virtual Learning Platform/Adobe, IVLP

Is this a new system?

No

Is there a PCLIA for this system?

Yes

What is the full name, acronym, and milestone of the most recent PCLIA?

IVLP, # 7577

What is the approval date of the most recent PCLIA?

3/9/2023

Changes that occurred to require this update:

Were there other system changes not listed above?

Yes

What were those changes?

One being Michael Young as the owner of Adobe Connect, and the other change was to remove any instance of Adobe Connect being used by non-IRS external parties. This updated PCLIA removes external access to the application.

What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym.

User and Network Services (UNS)Governance Board

Current ELC (Enterprise Life Cycle) Milestones:

System Development/Milestone 4B

Is this a Federal Information Security Management Act (FISMA) reportable system?

Yes

GENERAL BUSINESS PURPOSE

What is the general business purpose of this system? Provide a clear, concise description of the system, application or database, the reason for the system, and the benefits to the IRS to use the information, and how the information will be used.

The Integrated Virtual Learning Platform (IVLP) Project initiative is to replace the current enterprise Saba Meeting 8.3.5 platform with Adobe Connect Meeting, which is a Software-As-A-Service (SaaS) solution hosted by CoSo, a third-party vendor, located in the Amazon Web Service (AWS) data centers. This will only be used as a Training Platform. The intent is to acquire a future-proof solution to meet the IRS Taxpayer First Act requirement to establish a continuous learning environment with new technology to create accessible, high-quality, and effective program to optimize the employee training experience. Adobe Connect Meeting will utilize single sign-on (SSO) authentication capabilities for IRS employees. The SSO capability will promote ease of use for IRS employees by eliminating the need to enter their HRConnect User/Employee ID and Password to login.

PII DETAILS

Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information: or any other type of Sensitive but Unclassified (SBU) information or PII such as information about IRS employees or outside stakeholders?

Yes

Does the system use, collect, receive, display, store, maintain, or disseminate Social Security Numbers (SSN's) or tax identification numbers (i.e., last 4 digits, etc.)?

No

Does this system use, collect, receive, display, store, maintain or disseminate other (non-SSN) PII (i.e., names, addresses, etc.)?

Yes

Specify the PII Elements:

Name
Phone Numbers
E-mail Address
Standard Employee Identifier (SEID)
Photographic Identifiers
Biometric Identifiers

Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?

Yes

Specify the types of SBU from the SBU Types List:

Official Use Only (OUO) or Limited Official Use (LOU) - Information designated as OUO or LOU is information that: is exempt under one of the statutory Freedom of Information Act exemptions; is prohibited by other laws or regulations; would significantly impede the agency in carrying out a responsibility or function; or would constitute an unwarranted invasion of privacy.

Proprietary Data - Business information that does not belong to the IRS.

Are there other types of SBU/PII used in the system?

No

Cite the authority for collecting SBU/PII (including SSN if relevant).

PII for personnel administration is 5 USC

Has the authority been verified with the system owner?

Yes

BUSINESS NEEDS AND ACCURACY

Explain the detailed business needs and uses for the SBU/ PII, and how the SBU / PII is limited only to that which is relevant and necessary to meet the mission requirements of the system. If SSNs (or tax identification numbers) are used, explicitly explain why use of SSNs meets this criteria. Be specific.

The business need is for Adobe Connect Meeting to utilize single sign-on (SSO) authentication capabilities for IRS employees. The SSO capability will use SEID to identify the user for authentication. This will only be used as a Training Platform. No FTI (Federal Tax Information) or SSN information will be used or shared for this application. SBU/PII will only be used when signing into this training platform by using SEID for SSO authentication (internal users).

How is the SBU/PII verified for accuracy, timeliness, and completion?

Employee PII is verified by Active Directory (AD).

PRIVACY ACT AND SYSTEM OF RECORDS

The Privacy Act requires Federal agencies that maintain a system of records to publish systems of records notices (SORNs) in the Federal Register for records from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence. The Privacy Act also provides for criminal penalties for intentional noncompliance.

Does your application or this PCLIA system pertain to a group of any record from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence? An identifier may be a symbol, voiceprint, SEID, or other personal identifier that is used to retrieve information.

Yes

Identify the Privacy Act SORN(s) that cover these records.

IRS 36.003   General Personnel and Payroll Records

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

Official Use Only

INCOMING PII INTERFACES

Does the system receive SBU/PII from other systems or agencies?

Yes

Does the system receive SBU/PII from IRS files and databases?

No

Does the system receive SBU/PII from other federal agency or agencies?

No

Does the system receive SBU/PII from State or local agency (-ies)?

No

Does the system receive SBU/PII from other sources?

No

Does the system receive SBU/PII from Taxpayer forms?

No

Does the system receive SBU/PII from Employee forms (e.g., the I-9)?

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

Yes

Does this system disseminate SBU/PII to other IRS Systems?

Yes

Identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name: Splunk
Current PCLIA: Yes
Approval Date: 1/27/2020
SA&A: No

Identify the authority.

5 U.S.C 301, 1302, 2951, 4118, 4308 and 4506 18 U.S.C 1030 (a) (2) (B) 26 U.S.C 7801 Executive Orders 9397 and 10561.

For what purpose?

To identify and track any unauthorized accesses to sensitive but classified information and potential breaches of unauthorized disclosures of such information.

Does this system disseminate SBU/PII to other Federal agencies?

No

Does this system disseminate SBU/PII to State and local agencies?

No

Does this system disseminate SBU/PII to IRS or Treasury contractors?

No

Does this system disseminate SBU/PII to other Sources?

No

PRIVACY SENSITIVE TECHNOLOGY

Does this system use social media channels?

No

Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.?

Yes

Briefly explain how the system uses the referenced technology.

Cameras may be used by instructors providing the training.

Does the system use cloud computing?

Yes

Is the cloud service provider (CSP) Federal Risk and Authorization Management Program (FedRAMP) certified?

Yes

Date Certified.

4/19/2021

Please identify the ownership of the CSP data.

IRS

Does the CSP allow auditing?

Yes

Who audits the CSP Data?

IRS

What is the background check level required for CSP?

Moderate

Is there a breach/incident plan on file?

Yes

Privacy laws (including access and ownership) can differ in other countries. This cloud will be Continental US (CONUS) only for:

Storage
Transmission
Maintenance

Does this system/application interact with the public?

No

INDIVIDUAL NOTICE AND CONSENT

Was/is notice provided to the individual prior to collection of information?

Yes

How is notice provided? Was the individual notified about the authority to collect the information, whether disclosure is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects on the individual, if any, if they decide not to provide all or any of the requested information?

The business units are responsible for notifications to individuals. The host of the Adobe Connect Meeting session will have the ability to record/transcript the session. When the recording/transcript feature is initialized, all attendees of the session will receive an on-screen notification stating that the session is now being recorded. And those attending that session will then be given the option to remain in or leave the meeting.

Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information?

Yes

Describe the mechanism by which individuals indicate their consent choice(s):

The individual can refuse to stay in a recorded session and leave the meeting.

How does the system or business process ensure 'due process' regarding information access, correction, and redress?

This will only be used as a Training Platform. Adobe Connect Meeting provides IRS personnel a mechanism to conduct virtual training for personnel within the IRS WAN (Wide Area Network). No FTI (Federal Tax Information) or SSN information will be used or shared for this application. There will be no file transfers using this application. Event creation will

be controlled by Human Capital Office's (HCO) the Virtual Learning System (VLS) department. Only 22 people will be able to create the training events. The host of the event will be monitoring who enters the event based on enrollments. Event hosts will be verifying participant access.

INFORMATION PROTECTION

Identify the owner and operator of the system (could be IRS owned and Operated; IRS owned, contractor operated; contractor owned and operated).

IRS Owned and Contractor Operated

The following people have access to the system with the specified rights:

IRS Employees

Users: Read Write

Managers: Read Write

System Administrators: Administrator

Developers: Read Write

IRS Contractor Employees

Contractor Users: Read Only

How is access to SBU/PII determined and by whom?

This will only be used as a Training Platform. No Federal Tax Information (FTI) will be used or shared on this application. Host (IRS user) will have profile in the cloud with attributes such as SEID, Email address, and Employee ID. Only admin will have access to user profiles. The admin and host roles will be approved by the BEARS entitlement system. Adobe Connect Meeting recordings/transcripts will be saved in the Cloud. The reports are only available to those with an Adobe Connect Meeting host license. Access is secured via IRS Personal Identification Verification (PIV) Card identification and authentication services.

RECORDS RETENTION SCHEDULE

Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) approved a Records Control Schedule (RCS, IRS Document 12990) for the retention and destruction of official agency records stored in this system?

Yes

How long are the records required to be held under the corresponding GRS or RCS, and how are they disposed of? In your response, please provide the GRS or RCS chapter number, the specific item number, and records series title.

All records will be deleted or destroyed in accordance with approved retention periods. Any records will be managed according to requirements under IRM 1.15.1 and 1.15.6.14 Use of Collaboration Tools and will be destroyed using IRS General Records Schedule (GRS) or IRS Records Control Schedule (RCS) and is coordinated with the IRS Records and Information Management (RIM) Program and IRS Records Officer. Log files will be maintained in accordance with GRS 3.2, item 030, or 031. In accordance with IRM 1.15.6.15 Use of Collaboration Tools: Note: This guidance does not cover voicemail/View mail or the exchange and sharing of real time information through Live Meeting, group training sessions or similar functions of a collaboration system. Business Unit creators are responsible for the official maintenance of training/presentation/briefing materials shared (or updated) using Live Meeting or screen shares. The instant messaging software server is not the recordkeeping repository for those documents, and copies maintained by meeting participants would be considered reference material eligible for destruction when no longer needed. The Business Unit initiating a Live Meeting or share session to conduct business must make a decision as to the most appropriate method for documenting the session, such as an audio recording or written minutes. All official meeting records including the agenda, minutes, handouts, presentation materials, and recordings, should be maintained outside the session by the host Business Unit in association with an approved disposition authority for that office.

SA&A OR ASCA

Has the system been through SA&A (Security Assessment and Authorization) or ASCA (Annual Security Control Assessment)?

In-process

When is the anticipated date of the SA&A or ACS completion?

8/18/2023

Describe the system's audit trail.

Our plan is to have Splunk integration with Adobe Connect Meeting in order to retrieve SAML and event/activity logs to meet the IRM 10.8.1.4.3.2 standards. This is also part of the ELC Process.

PRIVACY TESTING

Does the system require a System Test Plan?

Yes

Is the test plan completed?

No

When is the test plan scheduled for completion?

9/29/2023

Describe what testing and validation activities have been conducted or are in progress to verify and validate that the applicable Privacy Requirements (listed in header) have been met?

Because this is a Cloud managed service, we could only test our current use cases. Before being implemented to the enterprise environment, further testing will be completed. A proof of concept with approximately 30 testers was conducted using different use cases. Those results are in the IVLP share point folder.

SBU DATA USE

Does this system use, or plan to use SBU Data in Testing?

No

NUMBER AND CATEGORY OF PII RECORDS

Identify the number of individual records in the system for each category:

IRS Employees: 50,000 to 100,000

Contractors: Under 5,000

Members of the Public: Not Applicable

Other: No

CIVIL LIBERTIES

Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment?

No

Is the system information used to conduct 'data-mining' as defined in the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?

No

Will this system have the capability to identify, locate, and monitor individuals or groups of people?

No

Does computer matching occur?

No

ACCOUNTING OF DISCLOSURES

Does the system include or require disclosure of tax or employee information to anyone other than IRS employees in the performance of their duties, or to the person to whom the information pertains or to a 3rd party pursuant to a Power of Attorney, tax, or Privacy Act consent?

No