Date of Approval: **January 17, 2020**

PIA ID Number: **4451**

SYSTEM DESCRIPTION

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

Academic Professional and Corporate Testing System, AP&C

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?

PCLIA 1909

What is the approval date of the most recent PCLIA?

11/22/2016

Changes that occurred to require this update:

Expiring PCLIA

Were there other system changes not listed above?

No

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

Return Preparer Office

Current ELC (Enterprise Life Cycle) Milestones:

Operations & Maintenance (i.e. system is currently operational)

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

No

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 Academic Professional and Corporate (AP&C) Testing System is a web-based application that is used by tax return preparers who choose to take a certification exam in order to be certified as Enrolled Agent. The purpose of the AP&C system is to: Register and schedule a tax certification examination, administer the test, and communicate results to the IRS (eTrak Practitioner Module). The system is hosted externally to the IRS and accessed directly on an external site. There is a link to it from IRS.gov.

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.)?

Yes

What types of tax identification numbers (TIN) apply to this system?

Other Taxpayer Identification Number

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

Mailing address

Phone Numbers

E-mail Address

Date of Birth

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

Agency Sensitive Information Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission

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

Yes

Describe the other types of SBU/PII that are applicable to this system.

Special Enrollment Exam (SEE) questions and answers.

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

PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, & 6012e(a)

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.

PII is collected in order to verify the identity of individuals who take the Special Enrollment Exam.

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

On the test date, the individual is required to show the necessary identity documents that correspond with the test registrant proving they are indeed the individual who has scheduled the test.

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 37.009 Enrolled Agent and Enrolled Retirement Plan Agent 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?

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

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

Does the system receive SBU/PII from other sources?

Yes

Identify the source that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name: site
Transmission Method: users self-assert data on web registration page
ISA/MOU: No

Does the system receive SBU/PII from Taxpayer forms?

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

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: eTrak-Practitioner
Current PCLIA: Yes
Approval Date: 3/21/2017
SA&A: Yes
ATO/IATO Date: 1/1/2013

Identify the authority

Circular 230

For what purpose?

Required for IRS Enrolled Agent program. In order to transfer test results to the IRS for purposes of certifying Enrolled Agents.

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.?

No

Does the system use cloud computing?

No

Does this system/application interact with the public?

Yes

Was an electronic risk assessment (e-RA) conducted on the system/application?

Not Applicable

Please explain.

Commercial software product owned and operated by the contractor and provided to the IRS as a Managed Service, developed for a variety of commercial customers and leveraged by the IRS, also classified by IRS Cybersecurity as FISMA Non-reportable system, governed by the Contractor Security Assessment (CSA) yearly site visit. Last CSA successfully completed on 11/2/2018, results of security assessment available upon request.

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?

Individuals notified via on-screen notification and check-box.

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):

When registering for the exam, they must agree to the appropriate uses of information prior to continuing.

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

The system allows for due process. If information is entered incorrectly, the user has the ability to correct it.

INFORMATION PROTECTION

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

Contractor Owned and Operated

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

IRS Employees

Users: Read Only

Managers: Read Only

IRS Contractor Employees

Contractor Users: Read Write

Contractor Managers: Read Write

Contractor System Administrators: Administrator

Contractor Developers: Read Write

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

The Return Preparer Office (RPO) will identify authorized IRS personnel; Treasury Inspector General for Tax Administration will identify personnel in its organization that will have access and share that information with the RPO, their managers, etc.; on the vendor's side access will be determined by the vendor. Access to the data is determined by the manager based on a user's position and need-to-know. The vendor utilizes Active Directory (AD) to automate access control to the system and ensure compliance. Each account requires a unique user id and individual accounts are granted level of access through AD. A security administrator is assigned to monitor AD. IRS Cybersecurity assesses all required Access Controls from IRS Publication 4812 during the annual Contractor Security Assessment (CSA). FY2019 CSA was completed in Nov 2018.

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 housed in the Academic Professional and Corporate Testing System will be erased or purged from the system in accordance with approved retention periods. It is the official repository for data and documents, also has the National Archives approval to affect data disposition. Any records generated and maintained by the system will be managed according to requirements under IRM 1.15.1 and 1.15.6 and will be destroyed using IRS Records Control Schedule (RCS) 11 for IRS TAX PRACTITIONER ENROLLMENT, PROFESSIONAL RESPONSIBILITY, AND AGENT PRACTICES, Item 17a as published in Document 12990, and as coordinated with the IRS Records and Information Management (RIM) Program and IRS Records Officer.

SA&A OR ASCA

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

No

Is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements?

Yes

Describe the system's audit trail.

The system's audit & accountability Policy & Procedure is described in the Audit Trail Policy. Vendor uses an Audit Log which tracks the event , time stamp, and the source of the event. Audit log stores 90 days worth of online log files and indefinite offline. Vendor uses HPE Insight to provide alerts when audit records stop recording. The policies highlight that Prometric staff review the collection of audit log information. The Audit Log Manager provides highlights and report generation. All audit events are recorded with timestamps. The audit log configuration restricts access to appropriate personnel to view audit logs. No Federal Tax Information (FTI) is created, processed, or stored by the system. All audit security controls are assessed on site by IRS Cybersecurity each year during the Contractor Security Assessment (CSA). The most recent CSA for FY2019 was completed in November 2018 and identified that all audit security controls are currently being met with no findings identified. CSA results for all vendor audit controls available upon request.

PRIVACY TESTING

Does the system require a System Test Plan?

Yes

Is the test plan completed?

Yes

Where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)?

The entire operation is reviewed in detail annually as part of the Contractor Security Assessment (CSA) process performed by IRS Cybersecurity. These results are stored on the RPO secure SharePoint site.

Were all the Privacy Requirements successfully tested?

Yes

Are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved?

No

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?

Yearly assessments are performed, and results are documented in the Security Assessment Report (SAR). These results are stored on the Return Preparer Office (RPO)secure SharePoint site.

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: Under 50,000

Contractors: Under 5,000

Members of the Public: Under 100,000

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