NOTE: The following reflects the information entered in the PIAMS Website.

A. SYSTEM DESCRIPTION

Authority: Office of Management Budget (OMB) Memorandum (M) 03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 & PVR #10- Privacy Accountability and #21-Privacy Risk Management

Date of Approval: 03/24/2014 PIA ID Number: **800**

1. What type of system is this? Non-Major System

1a. Is this a Federal Information Security Management Act (FISMA) reportable system? No

2. Full System Name, Acronym, and Release/Milestone (if appropriate):

Electronic Candidate Exam Results Tracking System, eCerts

2a. Has the name of the system changed? No

If yes, please state the previous system name, acronym, and release/milestone (if appropriate):

3. Identify how many individuals the system contains information on

Number of Employees:	Not Applicable
Number of Contractors:	Not Applicable
Members of the Public:	Under 100,000

4. Responsible Parties:

NA

5. General Business Purpose of System

The IRS contracted AIRE to develop and administer the Enrolled Retirement Plan Agent Special Enrollment Examination (ERPA-SEE) on behalf of the Service. The ERPA-SEE is taken by individuals who are interested in becoming enrolled retirement plan agents and representing taxpayers before the IRS. Individuals may apply online to take the ERPA-SEE web version test at one of the AIRE-sponsored test sites. AIRE began administering the ERPA-SEE test during the month of January 2009. AIRE agrees to transmit the test results to IRS after they complete processing the individual exams. Beginning with the first testing window in January 2014, AIRE agrees to make transmissions on a daily basis. Test results consist of passing and failing results. Due process is provided outside of the system for the system by regulations governing these procedures.

6. Has a PIA for this system, application, or database been submitted previously to the Office of Privacy Compliance? (*If you do not know, please contact* *Privacy *and request a search*) No

6a. If Yes, please indicate the date the latest PIA was approved:

6b. If Yes, please indicate which of the following changes occurred to require this update.

- **System Change (1 or more of the 9 examples listed in OMB 03-22 applies) (refer to PIA Training Reference Guide for the list of system changes)**
- **System is undergoing Security Assessment and Authorization**

6c. State any changes that have occurred to the system since the last PIA

7. If this system has an Exhibit 53 or Exhibit 300 please provide the Unique Project Identifier (UPI) number (XXX-XX-XX-XX-XX-XXXX-XX). Otherwise, enter the word 'none' or 'NA'. NA

B. DATA CATEGORIZATION

Authority: OMB M 03-22 & PVR #23- PII Management

8. Does this system collect, display, store, maintain or disseminate Personally Identifiable Information (PII)? Yes

8a. If No, what types of information does the system collect, display, store, maintain or disseminate?

9. Indicate the category that best describes the source that provides or originates the PII collected, displayed, stored, maintained or disseminated by this system. Most common categories follow:

Taxpayers/Public/Tax Systems	No	
Employees/Personnel/HR Systems	No	
Other	Yes	*Other Source:* Practitioners (Enrolled Retirement Plan Agent Candidates)

---

10. Indicate all of the types of PII collected, displayed, stored, maintained or disseminated by this system. Then state if the PII collected is on the Public and/or Employees. Most common fields follow:

TYPE OF PII	Collected?	On Public?	On IRS Employees or Contractors?
Name	Yes	Yes	No
Social Security Number (SSN)	No	No	No
Tax Payer ID Number (TIN)	No	No	No
Address	Yes	Yes	No
Date of Birth	Yes	Yes	No

Additional Types of PII: No

PII Name	On Public?	On Employee?
	No	No

10a. Briefly describe the PII available in the system referred to in question 10 above.

1. Practitioner Name i. First Name ii. Middle Name iii. Last Name 2. Address i. Street Address ii. City iii. State iv. Zip Code v. Province vi. Country vii. County 3. Contact ID 4. PTIN 5. Date of Birth 6. Enrolled Date 7. Cancelled Date 8. Postponed Date 9. Completion date 10. Test Number 11. Test Date 12. Grade 13. Telephone Number 14. E-mail Address

If you answered Yes to Social Security Number (SSN) in question 10, answer 10b, 10c, and 10d.

10b. Cite the authority that allows this system to contain SSN's? (e.g. specific regulations, statutes, etc.)

10c. What alternative solution to the use of the SSN has/or will be applied to this system? (e.g. masking, truncation, alternative identifier)

10d. Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of Social Security Numbers on this system?

11. Describe in detail the system's Audit Trail. State what data elements and fields are collected. Include employee log-in information. If the system does not have audit capabilities, explain why an Audit Trail is not needed.

A formal audit plan is not needed as deemed by ESAT. But here is some high level auditing information: All log incidents are to be time-stamped in Greenwich Mean Time (GMT) to synchronize events across all time zones. CSIRC maintains firewall logs for a minimum period of six (6) months on a log analysis system. Archived data can be made available and extends the data retention period to six (6) years. CSIRC log data is available to CSIRC personnel only and may be provided to law enforcement personnel with valid jurisdiction. IRS Enterprise Operations maintains server and management logs and make logs available to IRS CSIRC on an as requested basis for the analysis of security events. AIRE is responsible for auditing application processes and user activities involved in the interconnection. Recorded activities include event type, date, and time of event, user identification, workstation identification, success, or failure of access attempts and security actions taken by system administrators or security officers. The logs are archived and maintained for thirty (30) days. The enterprise monitoring system used by AIRE for the system involved in this connection is Hewlett Packard OpenView, which monitors the logs from all production systems.

11a. Does the Audit Trail contain the Audit Trail elements as required in current IRM 10.8.3 *Audit Logging Security Standards*? Yes

---

12. What are the sources of the PII in the system? Please indicate specific sources:

a. IRS files and databases: No

If Yes, the system(s) are listed below:

No System Records found.

b. Other federal agency or agencies: No

If Yes, please list the agency (or agencies) below:

c. State and local agency or agencies: No

If Yes, please list the agency (or agencies) below:

d. Third party sources: No

If yes, the third party sources that were used are:

e. Taxpayers (such as the 1040): No

f. Employees (such as the I-9): No

g. Other: No **If Yes*, specify*:**

C. PURPOSE OF COLLECTION

Authorities: OMB M 03-22 & Internal Revenue Manual (IRM) 10.8.8, IT Security, Live Data Protection Policy & PVR #16, Acceptable Use

13. What is the business need for the collection of PII in this system? Be specific.

Register and track Practitioners for the IRS. In order to determine, if a Practitioner is deemed knowledgeable to practice before IRS, in order to represent Taxpayers.

D. PII USAGE

Authority: OMB M 03-22 & PVR #16, Acceptable Use

14. What is the specific use(s) of the PII?

To conduct Tax Administration	No
To provide Taxpayer Services	No
To collect Demographic Data	No
For employee purposes	No

		If other, what is the use?
Other:	Yes	To register practitioners for the IRS and the ERPA (Enrolled Retirement Plan Agent) program.

E. INFORMATION DISSEMINATION

Authority: OMB M 03-22 & PVR #14- Privacy Notice and #19- Authorizations

15. Will the information be shared outside the IRS? (for purposes such as computer matching, statistical purposes, etc.) No

15a. If yes, with whom will the information be shared? The specific parties are listed below:

	Yes/No	Who?	ISA OR MOU**?
Other federal agency (-ies)			
State and local agency (-ies)			
Third party sources			
Other:			

** Inter-agency agreement (ISA) or Memorandum of Understanding (MOU)

16. Does this system host a website for purposes of interacting with the public? Yes

17. Does the website use any means to track visitors' activity on the Internet? Yes

If yes, please indicate means:

	YES/NO	**AUTHORITY**
Persistent Cookies	No	
Web Beacons	No	
Session Cookies	Yes	
Other:	No	*If other, specify:*

F. INDIVIDUAL CONSENT

Authority: OMB M 03-22 & PVR #15- Consent and #18- Individual Rights

18. Do individuals have the opportunity to decline to provide information or to consent to particular uses of the information? No

18a. If Yes, how is their permission granted?

19. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action? Not Applicable

19a. If Yes, how does the system ensure "due process"?

20. Did any of the PII provided to this system originate from any IRS issued forms? No

20a. If Yes, please provide the corresponding form(s) number and name of the form.

Form Number **Form Name**

20b. If No, how was consent granted?

Written consent	No
Website Opt In or Out option	No
Published System of Records Notice in the Federal Register	Yes
Other:	No

G. INFORMATION PROTECTIONS

Authority: OMB M 03-22 & PVR #9- Privacy as Part of the Development Life Cycle, #11- Privacy Assurance, #12- Privacy Education and Training, #17- PII Data Quality, #20- Safeguards and #22- Security Measures

21. Identify the owner and operator of the system: Contractor Owned and Operated

21a. If Contractor operated, has the business unit provided appropriate notification to execute the annual security review of the contractors, when required?

22. The following people have use of the system with the level of access specified:

	Yes/No	Access Level
IRS Employees:	No	
Users		
Managers		
System Administrators		
Developers		
Contractors:	Yes	
Contractor Users		No Access
Contractor System Administrators		Read Write
Contractor Developers		Read Write
Other:	No	

If you answered yes to contractors, please answer 22a. *(All contractor/contractor employees must hold at minimum, a "Moderate Risk" Background Investigation if they have access to IRS owned SBU/PII data.)*

22a. If the contractors or contractor employees act as System Administrators or have "Root Access", does that person hold a properly adjudicated "High Level"background investigation? Yes

23. How is access to the PII determined and by whom?

The Return Preparer Office will identify authorized IRS personnel, TIGTA will identify who in their organization will have access and share that with the Return Preparer Office and CSRs, their managers, etc., on the Vendor side will be determined by the Vendor. This is still being defined within the Project Office

24. How will each data element of SBU/PII be verified for accuracy, timeliness, and completeness?

Each data item will be validated for accuracy, correctness and completeness as defined in the technical requirements. The provider must legally affirm the accuracy, timeliness, and completeness of the data submitted.

25. Are these records covered under the General Records Schedule (GRS), or have a National Archives and Records Administration (NARA) archivist approved a Record Control Schedule (RCS) for the retention and destruction of official agency records stored in this system? No

25a. If Yes, how long are the records required to be held under the corresponding RCS and how are they disposed of? In your response, please include the complete IRM number 1.15.XX and specific item number and title.

If No, how long are you proposing to retain the records? Please note, if you answered no, you must contact the IRS Records and Information Management Program to initiate records retention scheduling before you dispose of any records in this system.

eCert is unscheduled. A request for records disposition authority for eCert data and associated records is currently being drafted with the assistance of the IRS Records and Information Management (RIM) Program Office. When approved by the National Archives and Records Administration (NARA), disposition instructions for eCert inputs, system data, outputs and system documentation will be published in IRS Document 12990, Records Control

Schedule and item number to be determined. Until a schedule is established and approved, all records will be retained.

26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.

The ERPA Web site, developed by AIRE, will be housed on a dedicated server in a DMZ zone. DeMilitarized Zone – A middle ground between an organization's trusted internal network and an untrusted, external network such as the Internet. Also called a "perimeter network," the DMZ is a subnetwork (subnet) that may sit between firewalls or off one leg of a firewall. Organizations typically place their Web, mail and authentication servers in the DMZ. This configuration creates a barrier between the public-facing Web server and the database server to further reduce the possibility of unauthorized access to the personal information of the candidates. All servers will have sufficient processor and memory resources to provide superior performance. In addition, all servers will have storage configured in a RAID 5 configuration to provide hardware redundancy and reduce the potential for data loss or corruption in the event of drive failure. All servers will require a user ID and password to access the administration system. The administrator-level logon credentials for these servers will only be given to the AIRE IT Manager and Network Analyst. A special account with lower-level permissions will be created for the personnel who require access to the system for customizations and updates to the Web site and core database systems. Logging will be enabled on each server such that all logins to the server desktops will be captured in the event logs by name and time. In addition, logging will be enabled at the SQL server level such that all logins to the SQL database back end will be captured by username and time. All three servers will be connected via a gigabit switch to the collocation firewall for Internet access and security. In addition, there will be a highly secure, encrypted VPN tunnel from the collocation facility to the AIRE offices for remote access to the servers for routine maintenance and monitoring. This VPN tunnel will be locked to only allow access from specific IPs, and require a login and password as well, before permission will be granted to the systems. Further, it will employ 128-bit encryption algorithms to encrypt all traffic between the sites. Passwords will be required to be changed at least every 60 days, and will not be allowed to repeat the previous five passwords. Passwords will conform to the current military standards for complexity (15 characters, including at least two of each of upper and lower case letters, numbers and special characters).

26a. Next, explain how the data is protected in the system at rest, in flight, or in transition.

All data in flight or in transistion is secured through an encrypted VPN. Data at rest resides behind secure authentication protocols. (furhter details can be found in question 26.)

27. Has a risk assessment (e.g., SA&A) been conducted on the system to ensure that appropriate security controls have been identified and implemented to protect against known risks to the confidentiality, integrity and availability of the PII? No

28. Describe the monitoring/evaluating activities undertaken on a regular basis to ensure that controls continue to work properly in safeguarding the PII.

The website is scanned quarterly by Security Metrics to check against all known PII access methodologies and to ensure PCI compliance. Weaknesses are reported after each scan for attention / remediation.

29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 - *IT Security, Live Data Protection Policy*? Yes

29a. Has approval been received from the Office of Privacy Compliance to use Live Data in testing (*if appropriate)*? No

29b. If you have received permission from the Office of Privacy Compliance to use Live Data, when was the approval granted?

H. PRIVACY ACT & SYSTEM OF RECORDS

Under the statute, any employee who knowingly and willfully maintains a system of records without meeting the Privacy Act notice requirements is guilty of a misdemeanor and may be fined up to $5000.

Authority: OMB M 03-22 & Privacy Act, 5 U.S.C. 552a (e) (4) & PVR #13-Transparency

30. Are 10 or more records containing PII maintained/stored/transmitted through this system? Yes

31. Are records on the system retrieved by any identifier for an individual? (Examples of identifiers include but are not limited to Name, SSN, Photograph, IP Address) Yes

31a. If YES, the System of Records Notice(s) (SORN) published in the Federal Register adequately describes the records as required by the Privacy Act? Enter the SORN number and the complete name of the SORN.

SORNS Number	SORNS Name
Treasury/IRS 37.009	Enrolled Agent and Enrolled Retirement Plan Agent
Treasury/IRS 34.037	IRS Audit Trail and Security Records System

Comments

I. ANALYSIS

Authority: OMB M 03-22 & PVR #21- Privacy Risk Management

32. What choices were made or actions taken regarding this IT system or collection of information as a result of preparing the PIA?

Resulted in the removal of PII from the system (e.g., SSN use reduced/eliminated)	No
Provided viable alternatives to the use of PII within the system	No
New privacy measures have been considered/implemented	No
Other:	No

32a. If Yes to any of the above, please describe:

NA

View other PIAs on IRS.gov