Date of Approval: **March 29, 2022**

PIA ID Number: **6746**

SYSTEM DESCRIPTION

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

Electronic Signature Storage And Retrieval, ESSAR

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?

eSignature, ESSAR, MS3-4a

What is the approval date of the most recent PCLIA?

8/23/2019

Changes that occurred to require this update:

Expiring PCLIA

Were there other system changes not listed above?

Yes

What were those changes?

Name change from eSignature to Electronic Signature Storage And Retrieval (ESSAR)

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

eA3 Governance Board

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.

ESSAR serves the purpose of recording an electronic signature on IRS online documentation. ESSAR will be a standard enterprise common service providing the capabilities for client applications to save electronic signatures in a standardized format.

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?

Social Security Number (SSN)

List the approved Treasury uses of the SSN:

Legal/statutory basis (e.g., where collection is expressly required by statute)

Explain why the authorized use(s) above support the new or continued use of SSNs (or tax identification numbers).

Federal agencies require in administration of their activities a system of accounts which identifies each person individually. The use of IRS employee's SSNs are permissible for personnel administration according to 5 USC & Executive Order 9397.

Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN's (or tax identification numbers).

The Office of Management and Budget Circular A-130 requires that federal agencies develop a mitigation or elimination strategy for systems that use SSNs, which the Service continues to develop strategies to meet. An exception to that requirement is when the SSN is uniquely needed to identify a user's record.

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:

Internet Protocol Address (IP Address)

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

No

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

SSN for tax returns and return information is Internal Revenue Code Section 6109

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.

ESSAR stores electronic signatures for online IRS documents. Electronic signatures require the signee to be identified, and for the identifying information to be saved. The PII is limited to information that would appear in an electronic signature. The name and SSNs are used to uniquely identify the signer of the electronic signature. The Security Analysis and Audit System (SAAS) requires the source IP address for security analysis and auditing. SAAS recording is required for ESSAR service.

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

Taxpayers will have to be authenticated at an Electronic Authorization (eAuth) level of assurance 3 (LOA3) in accordance with National Institute of Standards and Technology Special Publication 800-63 revision 2.

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 00.001 Correspondence Files and Correspondence Control Files

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?

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: IRS Tax Pro Web application
Transmission Method: Service all (Tax Pro calls ESSAR service)
ISA/MOU: 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?

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?

No

INDIVIDUAL NOTICE AND CONSENT

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

No

Why not? If information is not collected directly from an individual, please discuss the factors considered in deciding to collect information from third party sources.

We do not interact with the individual. This is done at the client application, not our service.

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):

There is a checkbox in the client application indicating their intent to sign and a submit button that is only enabled when the checkbox is selected.

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

The user will validate their identity prior to the client application requesting an electronic signature be saved. All disputes would be handled by the client application, not ESSAR. All access to the electronic signature would be through the client application as the user does not have direct access to the ESSAR service.

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 Operated

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

IRS Employees

System Administrators: Administrator

Developers: Read Only

IRS Contractor Employees

Contractor Developers: Read Only

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

When an issue is discovered that needs to be corrected in production, the developers will access the database to ensure that specific entries are correct. Access is only provided during the troubleshooting and remediation of the issues to the developers and system administrators involved.

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?

No

You must work with the IRS Records and Information Management (RIM) Program Office to address records retention requirements before you dispose of any records in this system.

SA&A OR ASCA

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

Yes

What date was it completed?

2/2/2021

Describe the system's audit trail.

ESSAR will generate auditable event information per the Audit Worksheet and will be verbose (more information than typical logging) to identify nefarious activity. Auditable events are sent to Splunk, the enterprise automated tool.

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)?

SharePoint

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?

Testing is completed during the Development Phase. Because ESSAR is Agile, the testing will be determined during each sprint planning phase.

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: Not Applicable

Contractors: Not Applicable

Members of the Public: More than 1,000,000

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?

Yes

Does your matching meet the Privacy Act definition of a matching program?

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