Date of Approval: **June 16, 2021**

PIA ID Number: **6116**

**SYSTEM DESCRIPTION**

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

- eAuthentication, eAuth

**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?**

- eAuthentication, eAuth, PIAMS # 1530

**What is the approval date of the most recent PCLIA?**

7/10/2018

**Changes that occurred to require this update:**

- New Access by IRS employees or Members of the Public
- Expiring PCLIA

**Were there other system changes not listed above?**

Yes

**What were those changes?**

- Integration of additional IRS applications at the new LoA 2 security protection.

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

- Enterprise Life Cycle (ELC)
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?

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 objective of the eAuth system is to provide a core centralized security mechanism that integrates with the IRS infrastructure. The eAuth system provides a framework for identity-proofing and establishment of identities through credentialing in accordance with NIST SP 800-63 rev2 requirements, thereby providing security to the IRS applications it protects at multiple levels of assurances.

PII DETAILS

Does the system use, collect, 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, 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:

Another compelling reason for collecting the SSN

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

SSNs are only utilized when required (i.e., to enable the ID proofing service). For this reason, eliminating the use of SSNs is not applicable to eAuthentication.
Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN's (or tax identification numbers).

eAuthentication is expected to be sunset by December 2022 in favor of next generation framework. There is no current plan to work on replacing SSN as an Identity Verification key.

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
Standard Employee Identifier (SEID)
Internet Protocol Address (IP Address)
Financial Account Numbers
Tax Account Information

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.

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.

User ID and Password; Phone Number; Email Address; Secondary email address; IP Address; IP PIN Device ID; Standard Employee Identifier (SEID); Financial Account Information; Home Equity Loan Number; Auto Loan Number; Mortgage Loan Number; Student loan number

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.

Personally Identifiable Information (PII) data collected by the eAuthentication system is used to validate and authenticate individuals trying to access IRS services via the internet. The information is required to ensure only valid and approved IRS taxpayers and Non-Filers may access IRS services. The Freedom of Information Act (FOIA) and Privacy Act require identity proofing an individual. IRM 11.3.2.3.2 states current requirements for external authentication of users to IRS systems. It requires use of identity proofing elements such as taxpayer name, taxpayer address, taxpayer Social Security number and taxpayer date of birth and/or filing status. The other business use of the collected PII information is to conduct fraud analysis to identify and deter fraudulent usage of eAuth system by unauthorized users.

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

PII is submitted directly by the taxpayers and tax preparers. Once the user inputs their PII data, it gets validated against the IRS internal data source Integrated Customer Communications Environment (ICCE), validating they are who they say they are. If the information is not available for the users (Non-Filers), their PII data is validated against third party data service providers. Drop down menus and syntax requirements are enforced throughout the application to ensure the accuracy and completeness of data input.
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 24.030 Customer Account Data Engine Individual Master File
- IRS 24.046 Customer Account Data Engine Business Master File
- IRS 34.037 Audit Trail and Security 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?

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: External Data Service/Credit Bureaus
Transmission Method: In the case of Non-Filers Identity proofing. eAuth receives the standardized address back from the data service provider after successful verification
ISA/MOU: Yes

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: Integrated Customer Communications Environment (ICCE)
Current PCLIA: Yes
Approval Date: 2/20/2020
SA&A: Yes
ATO/IATO Date: 12/5/2018
System Name: Security Audit and Analysis System (SAAS)
Current PCLIA: Yes
Approval Date: 4/6/2020
SA&A: Yes
ATO/IATO Date: 4/29/2020

System Name: Secure Object Repository Delivery (SOR)
Current PCLIA: Yes
Approval Date: 5/31/2019
SA&A: Yes
ATO/IATO Date: 12/5/2018

System Name: Secure Access Digital Identity (SADI)
Current PCLIA: Yes
Approval Date: 6/10/2021
SA&A: No

Identify the authority.

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

For what purpose?

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

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?

Yes
Identify the other source(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name: External Data Services Provider  
Transmission Method: Secured channel via HTTPS  
ISA/MOU: Yes

Identify the authority.

Third party Data Service Vendors - Approved 3rd party data service providers. There is an ISA Interconnection Security Agreement) & MOU (Memorandum of Understanding) with the approved external vendors.

Identify the Routine Use in the applicable SORN (or Privacy Act exception).

The approved Interface Control Document (ICD), governs the infrastructure design used to handle proofing operations. All communications with the external data service provider is conducted with encrypted FIPS (Federal Information Processing Standard) compliant methods.

For what purpose?

For the Account Verify, one of the proofing types, IRS sends the external vendor identity and financial account information for Filers and Non-Filers. This includes SSN, Name, DOB and Address. Additional validated includes Credit Card Proofing - last 8 numeric digits. Auto Loan Proofing- auto loan number, Mortgage Proofing- mortgage loan number, student loan number and Home Equity Loan Number. For Phone Verification, we send the users phone number for matching with their identity. The data service provider conducts additional fraud checks for further validation. No PII data is stored permanently by the third-party data service provider.

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.

As a part of the identity verification process, the system uses mobile phone number for the address of record verification and for use as a second factor device.
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?

Yes

When was the e-RA completed?

3/21/2013

What was the approved level of authentication?

Level 1: Little or no confidence in the asserted identity's validity.

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?

Notice is provided on the IRS.gov website. Notice, consent and due process are provided via the IRS systems and their related tax forms instructions, and pursuant to 5 USC.

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):

Individuals can opt not to proceed with the online session. There is an alternate process available at the IRS to obtain the service the user is looking for. Notice, consent, and due process are provided via the IRS systems and their related tax forms instructions, and pursuant to 5 USC.
How does the system or business process ensure 'due process' regarding information access, correction, and redress?

The system will allow affected parties the opportunity to clarify or dispute negative information that could be used against them. Notice, consent and due process are provided via the IRS systems and their related tax forms instructions, and pursuant to 5 USC.

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 Write

Managers: Read Write

System Administrators: Read Write

Developers: Read Write

IRS Contractor Employees

Contractor Users: Read Write

Contractor Managers: Read Write

Contractor Developers: Read Write

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

Taxpayers who chose to utilize eAuthentication services and register with the system have write access to their own user profile only. eAuth system administration is performed by IRS Enterprise Operation Services (EOps) group and IRS Wage and Investment (W&I) Electronic Products and Services Support (EPSS). eAuth administration will be performed by IRS employees and/or contractors whose access to eAuth system is granted via the Online 5081 process. Access to the data is determined by the manager based on a user's position and need-to-know.
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.

The National Archives and Records Administration (NARA) approved the destruction of eAuthentication data (user profiles) 7 years, 6 months after account expiration (Job No. N1-58-12-6, approved 11/14/2012). These disposition instructions will be published in Records Control Schedule 17 for Information Technology (IRS Document 12990), Item 31 when next updated. As required under the IRS Enterprise Architecture, a plan will be developed to purge the eAuthentication datastore (or records repository) of records eligible for destruction in accordance with the Records Control Schedule, as well as IRS records management requirements in IRMs 1.15.3 (Disposing of Records) and 1.15.6 (Managing Electronic Records).

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?

6/30/2020

Describe the system's audit trail.

Seeking updated information - PII information collected by eAuth is sent to Integrated Customer Communications Environment (ICCE) system for Identity Verification. Auditing events of ICCE system is outside of eAuth boundary. eAuth is generating log files that are sent to the Security-1 Security Audit and Analysis System (SAAS) for handling and audit review. eAuthentication is following the appropriate audit trail elements pursuant to current Audit Logging Security Standards.
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)?

eAuthentication Documentation Library on DocIT

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?

Functional testing, Regression testing, Systems Acceptance testing

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: 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?

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