Date of Approval: **May 22, 2023**

PIA ID Number: **7876**

SYSTEM DESCRIPTION

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

ID.me In-Person Verification Study, N/A

Is this a new system?

Yes

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

Authentication Authorization Access (A3) Executive Governance Board

Current ELC (Enterprise Life Cycle) Milestones:

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 IRS is exploring other means for in-person identity verification to meet compliance of National Institute of Standards and Technology Special Publication (NIST SP) 800-63-3, Identity Assurance Level 2 (IAL2) levels. The purpose of this identity proofing system and the process is to test a Credential Service Provider's (CSPs) in-person proofing capability utilizing a kiosk and the IRS contracted ID.me, a Kantara certified credential service provider. ID.me will utilize their Identity Gateway (IDIG) and their sub-contracted vendor (Sterling) to facilitate this in-person identity proofing contract independently of the IRS. This benefits the IRS and the Taxpayer (TP) because there is face-to-face assistance, direct transfer and review of identity evidence, and higher levels of authentication. The process is multifaceted; the TP can self-register through the vendor website to create an account with the CSP, supply PII needed to perform identity verification which includes a "financial records check," and select an in-person identity verification session to attend. The CSP has many kiosk machines placed nationwide and utilizes a QR code, which enables an easy scan and sign-in process. The electronic event details are captured by the kiosk. (The session/appointment's date, time, and identity documents) Onsite proofing and visual inspection of identity evidence prove the taxpayer is who they claim to be. PII such as SSN, address, date of birth, phone number, and government issued IDs are needed to ensure the

taxpayer passes identity verification. The identity attributes used in Kantara Identity Assurance Level 2 (IAL2) process is then validated remotely by a CSP (ID.me). Identity attributes are recorded and captured as is the data transferred to the IRS. (Through the existing IRS Secure Access Digital Identity (SADI) infrastructure, integration and credentialling process.) The evidence captured varies depending on what the taxpayer has available but must meet and pass NIST 800-63A STRONG and FAIR requirements described in the verification section of this PCLIA. Once the IAL2 credential is confirmed, a subset of verified identity attributes, as determined by IRS, will be sent programmatically to the IRS (e.g., SSN, Address) provided the taxpayer consented to the transfer. At this point the transferred subset of attributes are IRS data. The IRS can then match the taxpayer's information with the IRS Taxpayer Protection Program record and input the necessary transaction codes to complete treatment. Retention of data gathered will be maintained, stored, and destroyed as per the contract with the contracted ID.me and will not be used in any way other than as specified in the contract of service. As a Kantara certified CSP, ID.me is required to store the individual's attributes to make the digital identity interoperable at a high level of assurance. ID.me retains records for the full duration the individual's account is active and an additional three years from the time of account deletion. Sterling retains the identity evidence scanned through the kiosk for thirty days from the time of capture.

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:

When there is no reasonable alternative means for meeting business requirements

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

SSNs are collected in order to achieve identity resolution in support of tax administration. They are used to ensure proper alignment of the individual identified with this process to the tax account associated with the SSN.

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. As indicated above and later in the verification section of this PCLIA, the use of an SSN is required for both the registration and the in-person process and therefore, at this time, there is no other means to eliminate the use of them.

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
Internet Protocol Address (IP Address)
Photographic Identifiers

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?

Yes

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

Images of identity evidence such as driver's license or passport are captured and returned to meet National Institute of Standards and Technology (NIST) IAL2 identity proofing requirements.

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.

The use of SBU/PII (SSN, Name, email and mailing address, DOB, photographic identifiers, and government issued IDs) are essential identity proofing elements, as defined by NIST 800-63-3, and are needed to ensure the applicant's identity can be verified and they pass identity verification at NIST (IAL2) levels. The SBU/PII elements will be used when the taxpayer opts-in and registers through the CSP vendor website. The QR code they were sent is specific to them and enables them to begin the in-person session. The previously submitted PII or "financial records check" data will be compared to the taxpayer's in-person identity evidence by an onsite proofing supervisor, who will also visually inspect documents to ensure completeness, authenticity, and validity of documents, at which point will scanned. The identity attributes will be verified using an approved and higher level of authentication, Kantara Identity Assurance Level 2 (IAL2) and then is validated remotely by a Trusted Referee (ID.me). Consent to share information is captured and allows for the transfer of their data to the IRS. Once the IAL2 credential is confirmed, a subset of verified identity attributes, as determined by IRS, will be sent programmatically to the IRS (e.g., SSN, Address) provided the taxpayer consented to the transfer. At this point the transferred subset of attributes are IRS data. The IRS can then match the taxpayer's information with the IRS Taxpayer Protection Program record and input the necessary transaction codes to complete treatment. Retention of data gathered prior to becoming IRS data will be maintained, stored, and destroyed as per the contract with the contracted ID.me and will not be used in any way other than as specified in contract of service. As a federally certified identity provider, ID.me is required to store the individual's attributes in order to make the digital identity interoperable at a high level of assurance.ID.me retains records for the full duration the individual's account is active and an additional three years from the time of account deletion. Sterling retains the identity evidence scanned through the kiosk for thirty days from the time of capture.

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

ID.me verifies and validates PII in accordance with NIST 800-63A IAL2 requirements. For in person verification this includes validity checks, which includes Conducting a financial record check for PII verification, Visual inspection by proofing supervisor that evidence contains matching PII, Visual inspection by proofing supervisor that the taxpayer matchings the image on their STRONG piece of evidence, Upload of taxpayer identity evidence into the kiosk which is sent directly to the CSP. The kiosk identity evidence is stored for 30 days prior to deletion. Review of the authenticity of the evidence by CSP Trusted Referees The identity evidence is received directly from the Taxpayer and is deemed reliable and accurate. The identity evidence is not altered in any way by the CSP.

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

IRS 34.037 Audit Trail and Security Records

IRS 42.021 Compliance Programs and Projects 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: Taxpayer
Transmission Method: Direct data entry by taxpayer
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?

Yes

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

No

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?

Yes

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

Organization Name: Sterling
Transmission Method: secure data transfer
ISA/MOU: Yes

Identify the authority.

6103 (p)(9) Disclosure to contractors and other agents, 6103(n) Certain other persons

For what purpose?

No

Did the contract include the appropriate 6103(n) clauses for tax return and return information, and Federal Acquisition Regulations privacy clauses?

No

Explain:

N/A

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: Customer's email
Transmission Method: email
ISA/MOU: No

Identify the authority.

6103 (p)(9) Disclosure to contractors and other agents, 6103(n) Certain other persons

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

IRS/Treasury SORN-042-021: Disclosure of returns and return information may be made only as provided by 26 U.S.C. 6103. Material covered by rule 6(e) of the Federal Rules of Criminal Procedure may be disclosed only as permitted by that rule. IRS/Treasury SORN-034.037: General Use, Disclosure of returns and return information may be made only as provided by 26 U.S.C. 6103 and (6) Disclose information to a contractor, including an expert witness or a consultant, hired by the IRS, to the extent necessary for the performance of a contract.

For what purpose?

To confirm id authentication process was successfully completed. To track correspondence with Taxpayer and IRS for the purpose of ID proofing, Authentication and Fraud Detection, to the extent necessary for the performance of a contract.

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?

Yes

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

Yes

Date Certified.

6/10/2021

Please identify the ownership of the CSP data.

Third Party

Does the CSP allow auditing?

Yes

Who audits the CSP Data?

IRS

What is the background check level required for CSP?

None

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 IRS will send a 5071C letter to all taxpayers eligible for the pilot with notification to call the Taxpayer Protection Program phone line for assistance. The phone assistor will advise the taxpayer of their option to complete in-person identity verification as part of their issue resolution. The taxpayer will be directed to the ID.me website. The privacy policy will be part of the ID.me web pages.

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):

All individuals have the right to decline to provide information. The taxpayer has the option of completing the authentication by visiting a TAC office. During the ID.me online verification process, the taxpayer has the option to exit at any time. For Taxpayer Protection Program, unless the taxpayer contacts IRS via one of these options, the return will not be processed.

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

The process and procedures used by the Taxpayer Protection Program are dictated by the Internal Revenue Manual guidelines. IRS policy allows individuals whose data is in the system the opportunity to clarify or dispute negative determinations through the appeals process.

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 Contractor Employees

Contractor Users: Read Only

Contractor Managers: Read Only

Contractor System Administrators: Administrator

Contractor Developers: Read Only

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

ID.me restricts access to information within its systems through security controls that manage role-based access and need to know. As a FedRAMP Moderate authorized CSP, these controls are reviewed by an external certified third-party assessor for conformance then results of that assessment provided to all government agencies using the ID.me service. Select verified identity attributes collected during identity verification will be sent to the IRS (e.g., SSN, Address) only with the taxpayer's consent. This information will be passed to the IRS via OpenID Connect (OIDC) through the existing IRS SADI infrastructure and integration.

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)?

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.

In accordance with FedRAMP, Kantara Initiative, and NIST SP 800-63-3, ID.me maintains controls that produce audit logs for the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes. For identity credentials, identity evidence, proofing actions, account details, statuses and related account metadata are retained for audit purposes.

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

This a ID.me owned and operated system and not subject to IRS System Test Plan currently.

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: 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