Date of Approval: **June 15, 2021**

PIA ID Number: **5889**

SYSTEM DESCRIPTION

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

ID.me, ID.me

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, and Access (A3) Executive Governance Board (EGB)

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 IRS Secure Access Digital Identity (SADI) program has requirements to modernize the current eAuth solution in order to meet compliance with NIST SP 800-63-3. To achieve the SADI vision, the program is performing a validation of design recommendations with a series of tests. The taxpayer will go to the id me site from irs.gov for the authentication. The IRS has contracted with ID.me to evaluate ID.me's Identity Gateway (IDIG) specifically to evaluate the user experience, pass-through rate, and false positives/negatives for users' identity proofing and authenticating to an external CSP Credential Service Provider. Confirm that the CSP is able to integrate and communicate with the IRS environment, and meet the performance load testing to identity proof, authenticate, and federate users for the IRS's citizen facing online services. The IRS has selected the Child Tax Credit User Portal to be the pilot. This will involve the Child Tax Credit User Portal users to knowingly consent and authorize the release of NIST SP 800-63-3 required identity attributes to ID.me. The users will be able to revoke ID.me's access to their data after the completion of the test by accessing their account settings in ID.me. ID.me is a Federal Identity, Credential and Access Management (FICAM) approved provider. This PCLIA is related to the SADI System PCLIA # 6170 and the Child Tax Credit User Portal PCLIA #6121.

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:

Interfaces with external entities that require 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).

The collection of SSN is required in order for ID.me to perform identity proofing at IAL2 in accordance with NIST SP 800-63-3. The NIST standards require the identity provider to perform a task known as identity resolution (see NIST 800-63A 5.1 https://pages.nist.gov/800-63-3/sp800-63a.html). Section 5.1 requires the identity provider and the government agency to use the smallest set of attributes possible to resolve to a unique individual. ID.me also performs sanctions checks to make sure that an individual is not on a sanctions list where government agencies and other organizations are prohibited from rendering services to the listed individual. Both of these checks currently require SSN as there is no ubiquitous identifier for Americans that can uniquely identify an individual. Section 8.1.1 addresses the use of SSN in particular. Driver's licenses and passports are not effective substitutes for an SSN as the vast majority of federal agencies do not have driver's license numbers associated with the Names and Dates of Birth of individuals in their database. As a result, the use of a driver's license, particularly a REAL ID, would potentially enable identity resolution to a unique individual for the Credential Service Provider, but, the Relying Party (RP in 8.1.1) or the government agency providing the application, does not have that same information on file for a given individual so identity resolution will fail for that user. For example, if ID.me sends over a data payload of Legal Name, Date of Birth (DOB), and Driver's License number to a federal agency, the agency will not be able to resolve that identity to one person and the records associated with that person because the federal agency does not have driver's license numbers (let alone current driver's license numbers) on file in combination with Name and DOB, so the agency cannot uniquely resolve the user's identity to ensure secure access to

PII. Passports have the same shortcoming. NIST 800-63A 8.1.1 notes that "the SSN may achieve identity resolution for RPs, in particular federal agencies that use SSNs to correlate a subscriber to existing records." SSNs are necessary for this reason.

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 memorandum Circular No. 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. The interaction between ID.me and the IRS requires the use of SSN to reliably identify the user. However, steps are taken to minimize display and transmissions of the SSN in any form not required to achieve the goals of the program. For this reason, eliminating the use of SSNs is not applicable.

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)
Passport Number
Photographic Identifiers
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:

Proprietary data Business information that does not belong to the IRS.

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

SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397

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.

ID.me will be collecting PII from taxpayers participating in the SADI Child Tax Credit User Portal Test 4 MVP pilot. Identity proofing elements, as defined by NIST 800-63-3, are needed to ensure the applicant's identity can be verified at NIST Identity Assurance Level 2 (IAL2).

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

ID.me verifies the accuracy, timeliness, and completeness of the data via audit logs and the use of advanced encryption both during transmission and while stored at rest. In order to meet NIST SP 800-63-3 requirements, the system verifies asserted PII against authoritative records, in this case credit agencies and mobile network operators (MNOs). The system only sends asserted PII and receives verification data from source. ID.me is unable to share any additional information within this document.

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 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: Credit and Financial Reporting Agencies
Transmission Method: Secure API
ISA/MOU: Yes

Organization Name: Document Verification
Transmission Method: Secure API
ISA/MOU: Yes

Organization Name: Mobile Network Operator
Transmission Method: Secure API
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: SADI Secure Access Digital Identity
Current PCLIA: Yes
Approval Date: 6/10/2021
SA&A: Yes
ATO/IATO Date: 6/16/2021

Identify the authority.

Federal Tax Administration Authority

For what purpose?

For the purpose of ID-Proofing, Authentication and Fraud Detection

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.?

Yes

Briefly explain how the system uses the referenced technology.

The use of mobile phones is required in order for the applicant to complete the IAL2 identity proofing process. Mobile phones are used as a piece of identity evidence themselves and to capture additional identity evidence (e.g., photo of government issued identification document). Geolocation can be gleaned from the Mobile Network Operators (MNOs) in the event of an investigation into a user. Biometrics are used in our LOA3, IAL2, and IAL2 + Liveness policies, leveraging best-of-breed facial matching technologies for comparing still (IAL2/ LOA3) or video (IAL2 + Liveness) selfies against the photo evidence uploaded by the user.

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?

3rd Party

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?

Yes

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

Not Applicable

Please explain.

ID.me is a Credential Service Provider (CSP) and provides various levels of assurance for its customers. The IRS that integrate with ID.me undergo an IRS digital risk assessment to determine the appropriate level of assurance that ID.me will provide.

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?

ID.me presents a consent screen that lists each data element the organization is requesting from the user. The user must provide explicit consent in order for ID.me to release their information to the organization.

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):

ID.me presents a consent screen that lists each data element the organization is requesting from them. The user must provide explicit consent in order for ID.me to release their information. If the user does not consent (declines), then no information is released to the organization.

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

ID.me believes that every user should have the ability to access and edit the Personally Identifiable Information and Sensitive Information you provide us. You may change email address and / or password by logging into your account and accessing the "my account" section of the site. You may update your Personally Identifiable Information or Sensitive Information by revoking access to the RP and reverifying, sending us an email at help@ID.me, or submitting an ID.me support ticket. For additional information see ID.me's privacy policy located at https://www.id.me/privacy ID.me does not assist in making determinations that may have an adverse impact on the users. While we support access, correction, and redress, participants are not subject to negative repercussions based on the results of their interactions with ID.me.

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 System Administrators: Administrator

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

ID.me employs role-based access controls (RBAC) to servers containing sensitive data. Authorization is done on a least privilege model with access changes requiring ticket and management approval. ID.me personnel is required to complete annual security awareness and privacy training. In addition, users who choose to utilize the ID.me identity proofing service and retain their account, have complete access and control over their own user profile and attributes.

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.

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 adheres to NARA's minimum records retention requirement of seven years and sometimes increases those requirements if state law, regulation, or agency policy requires a longer record retention period for audit purposes. GRS 3.2 Item 060/061-PKI administrative records-FBCA CAs.Destroy/delete when 7 years 6 months, 10 years 6 months, or 20 years 6 months old, based on the maximum level of operation of the CA, or when no longer needed for business, whichever is later. GRS 5.6 Item 120-Personal identification credentials and cards-Application and activation records-Destroy mandatory and optional data elements housed in the agency identity management system and printed on the identification card 6 years after terminating an employee or contractor's employment, but longer retention is authorized if required for business use.

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 adheres to a FICAM certified process, with last review completed in January 2020, and continued adherence to the requirements outlined in the NIST SP 800-63-3.

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 at this time.

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?

Yes

Describe the type of information derived from these efforts and the technical (e.g., audit trails) or other processes used to limit unauthorized monitoring.

This system has the ability to identify individuals and verify their identity in accordance with NIST SP 800-63-3 at IAL2. The information derived from these efforts is limited to what was specified in section 6.b.

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