

Date of Approval: **February 15, 2023**

PIA ID Number: **7545**

SYSTEM DESCRIPTION

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

Secure Access Digital Identity, SADI

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?

Secure Access Digital Identity, SADI, #7252

What is the approval date of the most recent PCLIA?

10/26/2022

Changes that occurred to require this update:

New Access by IRS employees or Members of the Public

Addition of Commercial Data or Sources

Were there other system changes not listed above?

No

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

e-Authentication, Authorizations & Access (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?

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 Secure Access Digital Identity (SADI) platform utilizes National Institute of Standards and Technology (NIST) Special Publication 800-63-3 compliant credential service provider (CSP) technology to enable people to securely access and use IRS online tools and applications. SADI utilizes CSP credentials to match users to their IRS account, pass the minimum amount of identifying data to internal applications, and connect users to information they are authorized to review. As part of the CSP selection process, the SADI project conducts an extensive battery of testing, auditing, and reviews to ensure our partners meet the rigors of federal regulations to secure personal information and protect individual privacy.

New functionality will be included for Login.gov and Kiteworks:

Login.Gov - Serves as a secondary source for credential servicing, ID.ME is the current source. Login.gov provides the public secure and private online access to participating government programs with one account for multiple agencies.

Kiteworks - Accellion's secure file sharing platform, Kiteworks, enables government agencies to securely connect their content to the people and systems that are part of their critical business systems processes, regardless of the applications that create that content or where it is stored, while maintaining the controls and visibility needed to demonstrate compliance.

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

Delivery of governmental benefits, privileges, and services

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

SSN is needed in the various applications for tax returns and return information. Also used for TIN/Name control validation. SADI does store SSNs.

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. The SADI system requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer at this time. System does utilize ITIN as other taxpayer identification numbers.

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:

Name

Mailing Address

Phone Numbers

E-mail Address

Date of Birth

Standard Employee Identifier (SEID)

Internet Protocol Address (IP Address)

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:

Agency Sensitive Information - Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission.

Proprietary Data - Business information that does not belong to the IRS.

Protected Information - Information which if modified, destroyed, or disclosed in an unauthorized manner could cause loss of life, loss of property or funds by unlawful means, violation of personal privacy or civil rights, gaining of an unfair procurement advantage by contractors bidding on government contracts, or disclosure of proprietary information entrusted to the Government.

Physical Security Information - Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities.

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.

SADI UNIVERSAL UNIQUE IDENTIFIER (UUID) The UUID is a unique random number generated by SADI for each individual taxpayer after they have been ID Proofed and authenticated by the Credential Service Provider (CSP). This UUID permanently remains with the taxpayer and is not shared with the CSP. irsShortID - A unique & random value generated by SADI used by tax professionals.

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.

SADI authentication is done by the Credential Service Provider (CSP) when it verifies that the claimant controls the necessary authenticators and is successful when the assertion is sent

to the IRS. Federation is the process that allows for the conveyance of authentication and subscriber attribute information from the CSP to the IRS. The IRS must support a variety of authenticator types to serve the largest possible taxpayer population. The requester is also required to provide proof of identity for verification. Name, address, and other identifying information is provided to assist in locating the requested information and responding to the request. A number of fields have input and user validation measures to reduce errors. The validated user fields allow access to the corresponding records matching the predefined data. SADI uses this identity data to connect users to information they are authorized to access.

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

Only asserted PII is received via the CSP system which has been verified against authoritative records, utilizing the CSP's proprietary processes. With that PII, the SADI platform will generate a universal unique identifier (UUID) for each individual taxpayer after they have been ID Proofed and authenticated by the Credential Service Provider (CSP). This UUID permanently remains with the taxpayer.

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

IRS 24.030 Customer Account Data Engine Individual Master File

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?

Yes

For each federal interface, identify the organization that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Name: Login.gov

Transmission Method: Secure Channel https

ISA/MOU: Yes

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: ID.me

Transmission Method: Secure channel https

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?

Yes

Identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name: IR Mod (Employee Portal Business and CSR)

Current PCLIA: Yes

Approval Date: 9/9/2022

SA&A: Yes

ATO/IATO Date: 12/9/2022

System Name: Digital Notice and Letters (DNL)

Current PCLIA: Yes

Approval Date: 9/16/2022

SA&A: Yes

ATO/IATO Date: 3/11/2021

System Name: Taxpayer Digital Communication (TDC) - Authenticated Web Chat

Current PCLIA: Yes

Approval Date: 9/1/2020

SA&A: Yes

ATO/IATO Date: 8/20/2019

System Name: TDC - Small Business / Self Employed (TDC - SB/SE)

Current PCLIA: Yes

Approval Date: 9/1/2020

SA&A: Yes

ATO/IATO Date: 8/20/2019

System Name: Identity Protection Personal Identification Number (IP PIN)

Current PCLIA: Yes

Approval Date: 12/16/2019

SA&A: Yes

ATO/IATO Date: 5/29/2019

System Name: TaxPro Account

Current PCLIA: Yes

Approval Date: 8/11/2020

SA&A: No

System Name: Child Tax Credit Update Portal (CTCUP)
Current PCLIA: Yes
Approval Date: 6/14/2021
SA&A: Yes
ATO/IATO Date: 6/9/2021

System Name: Splunk Enterprise
Current PCLIA: Yes
Approval Date: 1/27/2020
SA&A: Yes
ATO/IATO Date: 3/28/2017

System Name: Online Account (OLA)/WAES
Current PCLIA: Yes
Approval Date: 3/13/2019
SA&A: Yes
ATO/IATO Date: 11/24/2020

System Name: ID Verify
Current PCLIA: Yes
Approval Date: 8/6/2020
SA&A: Yes
ATO/IATO Date: 11/5/2019

System Name: GetTrans
Current PCLIA: Yes
Approval Date: 3/25/2020
SA&A: Yes
ATO/IATO Date: 5/17/2019

System Name: Online Payment Agreement (OPA)
Current PCLIA: Yes
Approval Date: 2/25/2022
SA&A: Yes
ATO/IATO Date: 3/11/2021

System Name: eServices
Current PCLIA: Yes
Approval Date: 11/16/2021
SA&A: Yes
ATO/IATO Date: 3/11/2021

System Name: TDC Secure Messaging
Current PCLIA: Yes
Approval Date: 9/1/2020
SA&A: Yes
ATO/IATO Date: 8/20/2019

System Name: TDC - Forms (F) 2848 & 8821 Intake
Current PCLIA: Yes
Approval Date: 9/1/2020
SA&A: Yes
ATO/IATO Date: 8/20/2019

System Name: TDC Appeals
Current PCLIA: Yes
Approval Date: 9/1/2020
SA&A: Yes
ATO/IATO Date: 8/20/2019

System Name: TDC Advance Pricing and Mutual Agreement (APMA)
Current PCLIA: Yes
Approval Date: 9/1/2020
SA&A: Yes
ATO/IATO Date: 8/20/2019

System Name: Foreign Account Tax Compliance Act (FATCA) QI
Current PCLIA: Yes
Approval Date: 11/8/2019
SA&A: Yes
ATO/IATO Date: 1/3/2022

System Name: ePostcard
Current PCLIA: Yes
Approval Date: 11/1/2021
SA&A: Yes
ATO/IATO Date: 3/15/2021

System Name: Modernized eFile (MeF)
Current PCLIA: Yes
Approval Date: 2/8/2022
SA&A: Yes
ATO/IATO Date: 2/9/2022

System Name: System 7.3 ACA Data Mart (Affordable Care Act)
Current PCLIA: Yes
Approval Date: 9/7/2022
SA&A: Yes
ATO/IATO Date: 3/3/2022

System Name: WAES IVES
Current PCLIA: Yes
Approval Date: 12/3/2021
SA&A: Yes
ATO/IATO Date: 9/30/2021

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.

As 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?

Yes

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

Yes

Date Certified.

11/3/2022

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?

Moderate

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?

No

When will the e-RA be completed?

12/31/2023

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).

IRS Owned and Operated

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

IRS Employees

Users: Read Only

Managers: Read Only

System Administrators: Read Only

Developers: Read Only

IRS Contractor Employees

Contractor Users: Read Write

Contractor Managers: Read Write

Contractor System Administrators: Read Write

Contractor Developers: Read Write

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

Taxpayers who chose to utilize SADI services and register with the system have write access to their own user profile only. SADI system administration is performed by IRS Enterprise Operation Services (EOps) group and IRS Wage and Investment (W&I) Electronic Products and Services Support (EPSS). SADI administration will be performed by IRS employees and/or contractors whose access to SADI system is granted via the Business Entitlement Access Request System (BEARS). 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 SADI 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 SADI 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?

8/23/2021

Describe the system's audit trail.

A complete audit trail of the use of the system is captured and includes every login, logoff, file access and database query. The system monitors for security risks and compliance violations to ensure that the use of the system takes place only for an approved purpose that is within the professional responsibility of each user. SADI 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)?

Collaborative Lifecycle Management (CLM)

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?

IRS conducts standard internal comprehensive functional and Integration testing on internal applications, such as SADI. All the customer configurable security controls will be implemented as intended and documented in the future SADI System Security Plan (SSP). IRS performs additional testing and auditing of CSPs, as detailed within privacy assessments specific to the CSP.

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