

Date of Approval: **June 04, 2019**

PIA ID Number: **3989**

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?

Yes

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

Authentication, Access, and Authorization (eA3)

Current ELC (Enterprise Life Cycle) Milestones:

Vision & Strategy/Milestone 0

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.

As part of the Internal Revenue Service (IRS)'s strategic effort, the Secure Access Digital Identity (SADI) project will implement an identity proofing and authentication solution that serves to protect taxpayer data and complies with the new National Institute of Standards and Technology (NIST) guidance. The SADI project will leverage modern tools and technologies to strengthen user experience and security. SADI is a major system sponsored by the IRS Identity Assurance Office (IAO) and Applications Development (AD) Identity & Access Management (IAM) that will deliver a modern Digital Identity technology platform and capabilities to protect IRS public facing applications. The platform will comply with new NIST SP 800-63-3 standards and provide a seamless and secure user experience for taxpayers accessing IRS online services. SADI is currently at the Agile Product Planning Phase. This phase corresponds to Milestone 2 waterfall methodology.

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

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)

SSN is needed for tax returns and return information.

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.

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)

Protection Personal Identification Numbers (IP PIN)

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 (SBUList)

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 SADI is used to ID proof 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 SADI system by unauthorized users.

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

The SADI Platform will use authentication to establish that someone attempting to access a protected resource is in control of the determined authenticators/credentials. ID Proofing and 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.

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 System

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

For 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?

Yes

Enter the files and databases:

System Name: Individual Master File (IMF)

Current PCLIA: Yes

Approval Date: 3/6/2017

SA&A: Yes

ATO/IATO Date: 9/22/2018

System Name: Return Review Program (RRP)

Current PCLIA: Yes

Approval Date: 10/6/2017

SA&A: Yes

ATO/IATO Date: 5/22/2018

System Name: Prisoner Reporting Tool (PRT)

Current PCLIA: Yes

Approval Date: 12/4/2017

SA&A: 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: Credential Service Providers (CSP)

Transmission Method: Secure Channels via HTTPS

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: Order a Transcript (OAT) formerly Short Term Transcript (ST-TRA)

Current PCLIA: Yes

Approval Date: 7/10/2018

SA&A: Yes

ATO/IATO Date: 5/22/2017

System Name: IRS2GO

Current PCLIA: Yes

Approval Date: 7/26/2017

SA&A: Yes

ATO/IATO Date: 10/20/2017

System Name: Get Transcript (GETTRANS)

Current PCLIA: Yes

Approval Date: 3/9/2017

SA&A: Yes

ATO/IATO Date: 1/16/2017

System Name: Where's My Refund?/Internet Refund Fact of Filing (WMR/IRFOF),

Current PCLIA: Yes

Approval Date: 2/13/2018

SA&A: Yes

ATO/IATO Date: 3/17/2017

System Name: Modernized Internet Employer Identification Number (MOD-IEIN),

Current PCLIA: Yes

Approval Date: 12/23/2016

SA&A: Yes

ATO/IATO Date: 6/27/2018

System Name: Federal Student Aid - Datashare (FSA-D)

Current PCLIA: Yes

Approval Date: 7/10/2018

SA&A: Yes

ATO/IATO Date: 6/4/2018

System Name: First Time Homebuyer Credit Lookup Tool (FTHBC)

Current PCLIA: Yes

Approval Date: 3/11/2019

SA&A: Yes

ATO/IATO Date: 1/8/2017

System Name: Where's My Amended Return? (WMAR)

Current PCLIA: Yes

Approval Date: 5/29/2019

SA&A: Yes

ATO/IATO Date: 5/1/2019

Identify the authority

Federal Tax Administration Authority

For what purpose?

For the purpose of Identity Proofing and 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 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?

Not Applicable

If Not Applicable, explain why not required.

The e-RA/DIRA assessment is used to determine what level an application needs to be protected by eAuthentication or SADI. The assessment is done for applications interfacing with eAuthentication or SADI, it would not be applicable to the protecting application itself.

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 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 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 Online 5081 process. Access to the data is determined by the manager based on a user's position and need-to-know.

RECORDS SCHEDULE

Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) archivist 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)?

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.

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?

No

When is the test plan scheduled for completion?

6/28/2019 12:00:00 AM

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?

Comprehensive functional and Integration testing will be conducted. All the customer configurable security controls will be implemented as intended and documented in the future SADI System Security Plan (SSP).

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?

Yes

Does the system have a process in place to account for such disclosures in compliance with IRC §6103(p) (3) (A) or Subsection (c) of the Privacy Act? Contact Disclosure to determine if an accounting is required.

Yes