

Date of Approval: **August 12, 2022**

PIA ID Number: **7102**

## **SYSTEM DESCRIPTION**

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

(EBR) TINEntry, (EBR) TINEntry

*Is this a new system?*

Yes

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

SBSE 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?*

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.*

TINEntry handles the input of the callers Taxpayer Identification Number (TIN), Social Security Number (SSN), and Employer Identification Number (EIN) on the Integrated Customer Communications Environment (ICCE) phone system. Once the TIN is entered, we may also do a data look up to see if the taxpayer matches certain conditions that require Customer Service Representative (CSR)/Agent intervention. If not, the caller is allowed to proceed into the interactive automated applications.

## **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

Statistical and other research purposes

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).*

Our system requires the callers SSN in order to provide services to the caller/taxpayer. Such as setting up installment agreements, using the caller's data to route them to an agent that can handle their specific issue in addition to other self-service applications tasks that provide data for the caller to complete tax returns and complete other IRS tasks the caller is trying to get information on.

*Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN's (or tax identification numbers).*

Application is currently in production and has been since early 2000s. There is no plan to eliminate the use of the SSN or EIN since that is required for the applications to function properly.

*Does this system use, collect, receive, display, store, maintain or disseminate other (non-SSN) PII (i.e., names, addresses, etc.)?*

No

*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?*

No

*Cite the authority for collecting SBU/PII (including SSN if relevant).*

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

Information by CI for certain money laundering cases may be 18 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.*

Collecting the SSN is vital in order to process the taxpayer and route them to an agent that can assist their specific conditions and allow the taxpayer to use many automated Phone applications. Also, other applications that interact with TINEntry require the SSN in order to perform some of their functions. Such as, setting up an installment agreement, Providing payoff amount to the taxpayer.

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

Taxpayer confirms their SSN when they enter it over the phone.

## **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 34.037 Audit Trail and Security Records  
IRS 00.001 Correspondence Files and Correspondence Control 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?*

Yes

*Enter the files and databases:*

System Name: Corporate Files Online

Current PCLIA: Yes

Approval Date: 5/1/2022

SA&A: Yes

ATO/IATO Date: 5/1/2022

System Name: Integrated Data Retrieval System

Current PCLIA: Yes

Approval Date: 5/1/2022

SA&A: Yes

ATO/IATO Date: 5/5/2022

*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?*

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?*

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.?*

No

*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?*

6/1/2022

*What was the approved level of authentication?*

Level 2: Some confidence in the asserted identity's validity  
Confidence based on Knowledge Based Authentication (Out of Wallet)

## **INDIVIDUAL NOTICE AND CONSENT**

*Was/is notice provided to the individual prior to collection of information?*

No

*Why not? If information is not collected directly from an individual, please discuss the factors considered in deciding to collect information from third party sources.*

Application was created prior to 1999 and the design at that time may not of had that requirement. TINEntry collects the callers TIN so that they can proceed with the actions they called to perform. Without the TIN the caller is not able to continue. They are told to call back when the information is available.

*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):*

They don't enter their TIN.

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

If the TIN is not provided the caller is disconnected and told to call back when they have the information available. We do Security Audit and Analysis System (SAAS) audit logging for any transaction that accesses PII data as well.

## **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*

System Administrators: Read Only

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

Access to the data by taxpayers is determined by the taxpayer entering valid shared secrets. Once they enter shared secrets and their data matches up with the IDRS/CFOL information to ensure that the information is correct, they are eligible to use the system. This is termed successful authentication.

## **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 disposition instructions for OPA inputs, system data, outputs, and system documentation in July 2012, under Job No. N1-58-11-11. All completed OPA sessions are updated to the Master File for official recordkeeping purposes. OPA disposition instructions published as pending in IRS Document 12990, Records Control Schedule 28 for Collections, item 158 will be updated to indicate approval upon next RCS 28 update. IDRS retains logs of all access of taxpayer records. All data and audit information is sent to SAAS application. NARA approved a 7-year retention of SAAS audit data under Job No. N1-58-10-22 (approved 4/5/2011). SAAS retention requirements will be incorporated into OPA records requirements.

## **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?*

5/5/2022

*Describe the system's audit trail.*

TINEntry will collect Management Information System (MIS) data related to the taxpayer's use of the application (e.g., how many hits encountered, how many taxpayers successfully transferred to an agent. In addition to MIS, in the current production environment, TINEntry sends all of its business layer outbound responses to SAAS through Application Messaging and Data Access Service (AMDAS) on the outbound queue. AMDAS provides a secure communication service between modernized components.

## **PRIVACY TESTING**

*Does the system require a System Test Plan?*

No

*Please explain why:*

System didn't require it.

## **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: 100,000 to 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