Date of Approval: **February 20, 2020**

PIA ID Number: **4510**

## SYSTEM DESCRIPTION

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

ICCE, View Transcript, TRA

*Is this a new system?*

No

*Is there a PCLIA for this system?*

No

*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.*

Integrated Customer Communications Environment (ICCE) provides customer service applications through toll-free telephone service and through Web Pages via the Internet. The toll-free telephone and Web Page services provides automated self-service applications that allow taxpayers to help themselves. View Transcript (TRA) provides users with the ability to request (telephonically) Tax Account and/or Tax Return Transcripts for user selected years. The users interact with TRA by responding to audio menus via Dual Tone Multi-Frequency (DTMF) sounds. They are limited to the past 4 Tax Years. The audio menus are provided in English and Spanish. TRA confirms user eligibility to request Transcripts by asking user for

their Social Security number (SSN) and then the House Number of the Street Address, which is compared to the stored data on file with the IRS. The availability of Transcript data (as input by user in response to menu prompts for Year and Type) is confirmed by accessing users Tax Account data. IRS data stores are read by TRA via Command Code ADDRS and Command Code LINDX. Successful requests for Transcripts are submitted to the eServices Transcript Delivery System (TDS) project for document generation and delivery via United States Postal Service. There is no SBU/PII contained (or stored) within the current tool.

## 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 IRS uses Taxpayer SSN as part of the key used to access Tax Account records of the Taxpayer. To provide Taxpayers with the product provided by TRA the Tax records must be accessed.

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

There is no mitigation strategy planned to stop or eliminate the use of Taxpayers SSN.

*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:*

Mailing address

*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*

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 IRS uses Taxpayer SSN and address as part of the key used to access Tax Account records of the Taxpayer. To provide Taxpayers with the product provided by TRA the Tax records must be accessed.

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

Taxpayer data is retrieved from IRS data stores. It is not within the scope of TRA to verify the accuracy, timeliness, and completeness of that data. TRA access the IRS data store in a read-only basis.

## 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

## 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: Individual Master File
Current PCLIA: Yes
Approval Date: 5/2/2017
SA&A: Yes
ATO/IATO Date: 9/5/2019

*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?*

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: eServices, Transcript Delivery System (TDS)
Current PCLIA: Yes
Approval Date: 12/18/2019
SA&A: Yes
ATO/IATO Date: 12/21/2019

*Identify the authority*

5 U.S.C. 301 and 26 U.S.C. 7801

*For what purpose?*

TDS creates the requested Transcript that is ultimately mailed to the Taxpayer.

*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.?*

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?*

12/12/2019

*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?*

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 notifies all individuals who file tax returns of such collection via the Privacy Act Notice in tax return instructions.

*Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information?*

No

*Why not?*

Taxpayer initializes access to the TRA application. Failure to provide required data will result in an unsuccessful interaction with Taxpayer.

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

If the Taxpayer responds with valid Street Address data as requested TRA will allow the user to make a request for Transcripts. Mailing of Transcripts is made to the Address of record found on IRS data stores. This ensures that if the caller is not the Taxpayer, it is not sent to the bad actor.

## 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

*IRS Contractor Employees*

Contractor System Administrators: Read Write

Contractor Developers: Read Only

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

External/Internal Users - no external users will have access to the system data. Note that no account data is returned to the user. The user puts in a request to have a transcript mailed to them and receive a status of the request. The Treasury Inspector General for Tax Administration can receive system data information by going through the proper channels. They do not have direct access to the system. Contractors, including Developers, will not have direct access to the production system or database. Contractors receive a completed Moderate risk background investigation for staff-like access approval. Only IRS System Administrators will have access to the production environment. However, Developers are available to help System Administrators troubleshoot technology problems. In these cases, the System Administrator will provide the necessary information to the Developer so he/she can assist with the problem, which is considered indirect access since the System Administrator will provide the Developer with the necessary information as opposed to the Developer being able to access it directly. Access to the data is determined by the manager based on a user's position and need-to-know. The manager will request a user to be added. They must submit the request via the Online 5081 process to request access to the System.

## 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.*

1040X master data file and associated records will be disposed of in accordance with Records Control Schedule (RSC) 29 for Tax Administration- Wage & Investment, Item 55-56. Recordkeeping copies of system data will be destroyed on or after January 16, 6 years after the end of the processing year (Job No. N1-058-95-001). The media that contain the data are degaussed and then destroyed. All records housed in the system will be erased or purged from the system at the conclusion of their retention period(s) as required under IRM 1.15.6. A control log is maintained containing the media label ID, date and method of destruction, and the signature of the person who destroyed the media.

## 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?*

5/29/2019

*Describe the system's audit trail.*

TRA writes logging records to the Management Information System (MIS) maintained by Integrated Customer Communication Environment (ICCE). These records are not deleted or archived.

## 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)?*

Test results are stored in DocIt (web-based document management system), an online secure repository.

*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?*

View Transcript is currently in the Operations and Maintenance phase of its lifecycle. Continuous Monitoring (now called Annual Security Control Assessment) occurs annually to ensure that controls remain in place to properly safeguard PII.

## 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?*

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