A. SYSTEM DESCRIPTION

Authority: Office of Management Budget (OMB) Memorandum (M) 03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 & PVR #10- Privacy Accountability and #21-Privacy Risk Management

Date of Approval: May 22, 2015 PIA ID Number: **897**

1. What type of system is this? Legacy

1a. Is this a Federal Information Security Management Act (FISMA) reportable system? Yes

2. Full System Name, Acronym, and Release/Milestone (if appropriate):

Short Term Transcript, ST-TRA

2a. Has the name of the system changed? No

3. Identify how many individuals the system contains information on

Number of Employees:	Not Applicable
Number of Contractors:	Not Applicable
Members of the Public:	Over 1,000,000

4. Responsible Parties: N/A

5. General Business Purpose of System

ST-TRA is used by the public to order copies of Account and/or Return transcripts - Orders are fufilled via mail to the user's address of record - Users may also obtain Form 4506 that may be used to order a copy of a tax return or one of several transcripts types - Due process for any errors in transcript information is available pursuant to 26 USC.

6. Has a PIA for this system, application, or database been submitted previously to the Office of Privacy Compliance? (*If you do not know, please contact* *Privacy *and request a search*) Yes

6a. If **Yes**, please indicate the date the latest PIA was approved: 10/4/2010

6b. If **Yes**, please indicate which of the following changes occurred to require this update.

- System Change (1 or more of the 9 examples listed in OMB 03-22 applies) (refer to PIA Training Reference Guide for the list of system changes) No
- System is undergoing Security Assessment and Authorization No

6c. State any changes that have occurred to the system since the last PIA

N/A

7. If this system has an Exhibit 53 or Exhibit 300 please provide the Unique Project Identifier (UPI) number (XXX-XX-XX-XX-XX-XXXX-XX). Otherwise, enter the word 'none' or 'NA'. NA

B. DATA CATEGORIZATION

Authority: OMB M 03-22 & PVR #23- PII Management

8. Does this system collect, display, store, maintain or disseminate Personally Identifiable Information (PII)? Yes

9. Indicate the category that best describes the source that provides or originates the PII collected, displayed, stored, maintained or disseminated by this system. Most common categories follow:

Taxpayers/Public/Tax Systems	Yes	
Employees/Personnel/HR Systems	No	
		Other Source:
Other	No	

10. Indicate all of the types of PII collected, displayed, stored, maintained or disseminated by this system. Then state if the PII collected is on the Public and/or Employees. Most common fields follow:

TYPE OF PII	Collected?	On Public?	On IRS Employees or Contractors?
Name	No	No	No
Social Security Number (SSN)	Yes	Yes	No
Tax Payer ID Number (TIN)	Yes	Yes	No
Address	Yes	Yes	No
Date of Birth	Yes	Yes	No

Additional Types of PII: No

10a. What is the business purpose for collecting and using the SSN ?

Authenticate User Identity and verify transcript is available prior to allowing order.

10b. Cite the authority that allows this system to contain SSN's? (e.g. specific regulations, statutes, etc.)

IRC 6109

10c. What alternative solution to the use of the SSN has/or will be applied to this system? (e.g. masking, truncation, alternative identifier)

N/A

10d. Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of Social Security Numbers on this system?

N/A

Describe the PII available in the system referred to in question 10 above.

ST-TRA is not a database. Data entered by the user is not retrievable once it is submitted.

11. Describe in detail the system's audit trail. State what data elements and fields are collected. Include employee log-in information. If the system does not have audit capabilities, explain why an audit trail is not needed.

ST-TRA audit data is captured by the Security Audit and Analysis System (SAAS). Audit trail logging for the application is sent to SAAS via Application Messaging and Data Access Services (AMDAS) regarding the success or failure of for each transaction that reaches the back-end.authentication of the user. The SSN, TIN type, File SourceCode, Date of Birth, Street Address and Zip Code are extracted from the National Account Profile (NAP) and the National Account Index (NAI) on a Read Only basis. The information entered by the user is captured for audit trail purposes. These Audit trails are for internal use and are closely guarded. They are only available to IRS employees who follow the proper procedures to gain access to them, which is by going through the OL5081 process. A manager must approve the OL5081 request and then an administrator will grant the access if the person is authorized by the organization to view the reports.

11a. Does the audit trail contain the audit trail elements as required in current IRM 10.8.3 *Audit Logging Security Standards*? Yes

12. What are the sources of the PII in the system? Please indicate specific sources:

a. IRS files and databases: Yes

If **Yes**, the system(s) are listed below:

System Name	Current PIA?	PIA Approval Date	SA & A?	Authorization Date
National Account Profile	No		No	
National Account Index	No		No	
Transcript Delivery System	No		No	
Security Audit and Analysis System	No		No	

b. Other federal agency or agencies: No

c. State and local agency or agencies: No

d. Third party sources: No

e. Taxpayers (such as the 1040): No

f. Employees (such as the I-9): No

g. Other: No

C. PURPOSE OF COLLECTION

Authorities: OMB M 03-22 & Internal Revenue Manual (IRM) 10.8.8, IT Security, Live Data Protection Policy & PVR #16, Acceptable Use

13. What is the business need for the collection of PII in this system? Be specific.

The ST-TRA application only asks for relevant information to authenticate the taxpayer requesting the service, and uses the module list to verify the transcript is available prior to ordering it.

D. PII USAGE

Authority: OMB M 03-22 & PVR #16, Acceptable Use

14. What is the specific use(s) of the PII?

To conduct tax administration	No	
To provide taxpayer services	Yes	
To collect demographic data	No	
For employee purposes	No	
		If other, what is the use?
Other:	No	

E. INFORMATION DISSEMINATION

Authority: OMB M 03-22 & PVR #14- Privacy Notice and #19- Authorizations

15. Will the information be shared outside the IRS? (for purposes such as computer matching, statistical purposes, etc.) No

16. Does this system host a website for purposes of interacting with the public? Yes

17. Does the website use any means to track visitors' activity on the Internet? No

F. INDIVIDUAL CONSENT

Authority: OMB M 03-22 & PVR #15- Consent and #18- Individual Rights

18. Do individuals have the opportunity to decline to provide information or to consent to particular uses of the information? Not Applicable

19. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action? Yes

19a. If **Yes**, how does the system ensure “due process”?

The Taxpayer Bill of Rights publication 1 at http://core.publish.no.irs.gov/pubs/pdf/p1--2014-12-00.pdf outlines the baseline for 'due process' that business follows. Due process is not applicable to the public in general as the system does not "use" the event information to interact with the tax paying public in any way. IRS employees and contractors using IRS email and web services may face disciplinary action for the misuse of SSNs. All IRS employees will be given the opportunity to defend their actions before a final determination is made. Contractor employees will be afforded any rights granted within the regulations that cover the specific contract they are working under. The system will allow affective parties the opportunity to clarify or dispute negative information that could be used against them. Due process is provided pursuant to 5 USC.

20. Did any of the PII provided to this system originate from any IRS issued forms? No

20b. If **No**, how was consent granted?

Written consent	No
Website Opt In or Out option	Yes
Published System of Records Notice in the Federal Register	Yes
Other:	No

G. INFORMATION PROTECTIONS

Authority: OMB M 03-22 & PVR #9- Privacy as Part of the Development Life Cycle, #11- Privacy Assurance, #12- Privacy Education and Training, #17- PII Data Quality, #20- Safeguards and #22- Security Measures

21. Identify the owner and operator of the system: IRS Owned and Operated

22. The following people have use of the system with the level of access specified:

	Yes/No	Access Level
IRS Employees:	Yes	
Users		No Access
Managers		No Access
System Administrators		Read Write
Developers		Read Only
Contractors:	Yes	
Contractor Users		No Access
Contractor System Administrators		No Access
Contractor Developers		No Access
Other:	No	

22a. If the contractors or contractor employees act as System Administrators or have “Root Access”, does that person hold a properly adjudicated “High Level”background investigation? Yes

23. How is access to the PII determined and by whom?

Access to this data is determined by business need and is requested via the Online (OL) 5081 system. The SAs and DBAs will first receive approval to access the data by their manager and then the OL-5081 is approved by the business owner or designee per IRS policy.

24. How will each data element of SBU/PII be verified for accuracy, timeliness, and completeness?

This validation process verifies the accuracy and completeness of the information input by the taxpayer in accordance with the business rules. It is worth noting that the only validation ST-TRA performs is a validation of the taxpayer’s SSN, TIN type, File Source Code, Date of Birth, Street Address and Zip Code against IRS records in the National Account Profile (NAP) to authenticate the applicant. ST-TRA passes the TIN entered by the taxpayer to NAP. If the information matches IRS records, the request process will proceed. If the information does not match

IRS records, the record will reject back to the taxpayer for correction and re-submission. If the taxpayer cannot correct the information within three attempts, he/she will be given an error page and their session will end.

25. Are these records covered under the General Records Schedule (GRS), or have a National Archives and Records Administration (NARA) archivist approved a Record Control Schedule (RCS) for the retention and destruction of official agency records stored in this system? Yes

25a. If **Yes**, how long are the records required to be held under the corresponding RCS and how are they disposed of? In your response, please include the complete IRM number 1.15.XX and specific item number and title.

The Short Term Transcript system is unscheduled. The RIM Office will work with the system owner to ensure that an approved retention schedule is drafted and submitted to the National Archives and Records Administration (NARA) for review and approval.

26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.
The information entered by the user is captured for audit trail purposes. Audit trails are for internal use and are closely guarded. They are only available to IRS employees who follow the proper procedures to gain access to them, which is by going through the OL5081 process. A manager must approve the OL5081 request and then an administrator will grant the access if the person is authorized by the organization to view the reports.

26a. Next, explain how the data is protected in the system at rest, in flight, or in transition.

NA

27. Has a risk assessment (e.g., SA&A) been conducted on the system to ensure that appropriate security controls have been identified and implemented to protect against known risks to the confidentiality, integrity and availability of the PII? No

28. Describe the monitoring/evaluating activities undertaken on a regular basis to ensure that controls continue to work properly in safeguarding the PII.

N/A

29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 - *IT Security, Live Data Protection Policy*? Not Applicable

H. PRIVACY ACT & SYSTEM OF RECORDS

Under the statute, any employee who knowingly and willfully maintains a system of records without meeting the Privacy Act notice requirements is guilty of a misdemeanor and may be fined up to $5000.

Authority: OMB M 03-22 & Privacy Act, 5 U.S.C. 552a (e) (4) & PVR #13-Transparency

30. Are 10 or more records containing PII maintained/stored/transmitted through this system? Yes

31. Are records on the system retrieved by any identifier for an individual? (Examples of identifiers include but are not limited to Name, SSN, Photograph, IP Address) Yes

31a. If **YES**, the System of Records Notice(s) (SORN) published in the Federal Register adequately describes the records as required by the Privacy Act? Enter the SORN number and the complete name of the SORN.

SORN Number	SORN Name
IRS 24.030	CADE/Individual Master File
IRS 34.027	IRS Audit Trail and Security Records System
IRS 24.046	Business Master File

I. ANALYSIS

Authority: OMB M 03-22 & PVR #21- Privacy Risk Management

32. What choices were made or actions taken regarding this IT system or collection of information as a result of preparing the PIA?

Resulted in the removal of PII from the system (e.g., SSN use reduced/eliminated)	No
Provided viable alternatives to the use of PII within the system	No
New privacy measures have been considered/implemented	No
Other:	No