A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Tax Return Database, TRDB

2. Is this a new system? No

   2.a. If **no**, is there a Privacy Civil Liberties Impact Assessment (PCLIA) for this system?   Yes

   If **yes**, enter the full name, acronym, and milestone of the most recent PCLIA.

   Tax Return Database (TRDB), MS4b - PCLIA #1403

   Enter the approval **date** of the most recent PCLIA.   11/06/2015

   If **yes** Indicate which of the following changes occurred to require this update (check all that apply).

No   Addition of Personally Identifiable Information (PII) (PII is any information that is linked or linkable).
No   Conversions
No   Anonymous to Non-Anonymous
No   Significant System Management Changes
No   Significant Merging with Another System
No   New Access by IRS employees or Members of the Public
No   Addition of Commercial Data / Sources
No   New Interagency Use
No   Internal Flow or Collection
Yes   Expiring PCLIA

   Were there other system changes not listed above?   No

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

Corporate Data Domain Governance Board (CPDGB)

3.a. Check the current Enterprise Life Cycle (ELC) Milestones (select all that apply).

   No   Vision & Strategy/Milestone 0
   No   Project Initiation/Milestone 1
   No   Domain Architecture/Milestone 2
   No   Preliminary Design/Milestone 3
   No   Detailed Design/Milestone 4A
   Yes   System Development/Milestone 4B
   No   System Deployment/Milestone 5
   Yes   Operations & Maintenance (i.e., system is currently operational)

4. Is this a Federal Information Security Management Act (FISMA) reportable system?   No

A.1 General Business Purpose

5. 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.

TRDB is a mainframe-based database application that assists the Wage & Investment Division in maintaining electronic tax return records and is the authoritative data store for electronically filed tax returns for tax years 1998 to present. TRDB receives the original tax returns as filed by the taxpayers from multiple Current Production Environment electronic filing systems. In addition, TRDB interfaces with Error Resolution System (ERS) to receive corrections to taxpayer submitted data, ERS processing statuses and processing information. ERS is not part of the TRDB accreditation boundary. The TRDB system also receives data perfection corrections to these returns prior to the return being posted to the Individual Master File or Business Master File and these corrections are stored on TRDB for subsequent research.

B. PII DETAIL

6. Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any type of Sensitive but Unclassified (SBU) or Personally Identifiable Information (PII)?
Yes

> 6.a. If **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

> If **yes**, check all types of tax identification numbers (TIN) that apply to this system:

Yes	Social Security Number (SSN)
No	Employer Identification Number (EIN)
No	Other Taxpayer Identification Number

> If SSNs apply, which of the following approved Treasury uses of the SSNs applies:

No	Security background investigations
Yes	Interfaces with external entities that require the SSN
Yes	Legal/statutory basis (e.g. where collection is expressly required by statute)
Yes	When there is no reasonable alternative means for meeting business requirements
Yes	Statistical and other research purposes
No	Delivery of governmental benefits, privileges, and services
No	Law enforcement and intelligence purposes
Yes	Another compelling reason for collecting the SSN

> Explain why one or more of the eight authorized uses above support the new or continued use of SSNs.

> The information stored in TRDB is stored by SSN and TIN. All command codes research is based upon SSN and TIN.

> 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 alternate method to the use of SSN and TIN. We cannot cross reference to SSN and TIN in any other method. Until such method is formed there is no mitigation strategy.

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

If **yes**, specify the information.

Selected	PII Element
Yes	Name
Yes	Mailing address
Yes	Phone Numbers
Yes	E-mail Address
Yes	Date of Birth
Yes	Place of Birth
No	Standard Employee Identifier (SEID)
Yes	Mother's Maiden Name
Yes	Protection Personal Identification Numbers (IP PIN)
Yes	Internet Protocol Address (IP Address)
No	Criminal History
Yes	Medical Information
Yes	Certificate or License Numbers
Yes	Vehicle Identifiers
No	Passport Number
Yes	Alien Number
Yes	Financial Account Numbers
No	Photographic Identifiers
No	Biometric Identifiers
Yes	Employment Information
Yes	Tax Account Information
Yes	Centralized Authorization File (CAF)

6.c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates?   Yes

If **yes**, select the types of SBU

Selected	SBU Name	SBU Description
No	Agency Sensitive Information	Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission
No	Procurement sensitive data	Contract proposals, bids, etc.
Yes	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.
No	Proprietary data	Business information that does not belong to the IRS
Yes	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
No	Physical Security Information	Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities
Yes	Criminal Investigation Information	Information concerning IRS criminal investigations or the agents conducting the investigations.

6.d. Are there other types of SBU/PII used in the system?   No

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

Yes	PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)
Yes	SSN for tax returns and return information is Internal Revenue Code Section 6109
No	SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
No	PII for personnel administration is 5 USC
No	PII about individuals for Bank Secrecy Act compliance 31 USC
No	Information by CI for certain money laundering cases may be 18 USC

6.f. Has the authority been verified with the system owner?   Yes

---

B.1 BUSINESS NEEDS AND ACCURACY

7. 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 PII collected in this system is used in the Internal Revenue Service (IRS) tax administration initiatives and strategies to: validate errors on tax returns, assess the correct tax and to aid in the compliance efforts of IRS revenue officers, tax examiners and field agents. The PII collected is also used to produce tax return transcripts requested by the taxpayers and their authorized representatives to support voluntary tax compliance.

8. How is the SBU/PII verified for accuracy, timeliness, and completeness?

Accuracy: TRDB interfaces with ERS to receive corrections to taxpayer submitted data, computer generated fields that differ from taxpayer submitted data, ERS processing statuses and processing information. Timeliness: Tax return data within TRDB is used to review filed tax returns to validate errors or for other purposes based upon field functions by IRS employees such as IRS revenue officers, tax examiners, and field agents. These users have read-only access to the data files queried within the TRDB. Completeness: The original return submitted by the taxpayer and the corrections are stored in the TRDB relational database system and are maintained for a minimum period of 10 years.

C. 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.

9. 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

If **yes**, enter the SORN number(s) and the complete the name of the SORN(s).

<div align="center">SORNS Name</div>

SORNS Number
IRS 24.046	Customer Account Data Engine Business Master File
IRS 24.030	Customer Account Data Engine Individual Master File
IRS 34.037	Audit Trail and Security Records System
IRS 22.062	Electronic Filing Records

*IRS is required to have a published Privacy Act system of records in the Federal Register. Please identify the Privacy Act SORN(s) that cover these records. If you need additional assistance identifying the correct SORNs please email *Privacy.*

D. RESPONSIBLE PARTIES

10. Identify the individuals for the following system roles. ## Official Use Only

---

E. INCOMING PII INTERFACES

11. Does the system receive SBU/PII from other system or agencies?   Yes

    11.a. If **yes**, does the system receive SBU/PII from IRS files and databases?   Yes

    If **yes**, enter the files and databases.

System Name	Current PCLIA	Approval Date	SA&A?	Authorization Date
Individual Master File	Yes	03/06/2017	Yes	11/04/2016
Generalized Mainline Framework	Yes	11/28/2017	Yes	07/20/2012
Modernized Tax Return Database	Yes	11/06/2015	No	
Business Master File	Yes	08/27/2018	Yes	01/29/2018
Integrated Data Retrieval System	Yes	08/29/2017	Yes	12/21/2016
Error Resolution System	Yes	12/28/2017	Yes	02/14/2012

    11.b. Does the system receive SBU/PII from other federal agency or agencies?   No

    11.c. Does the system receive SBU/PII from State or local agencies?   No

    11.d. Does the system receive SBU/PII from other sources?   No

11.e. Does the system receive SBU/PII from **Taxpayer** forms?   Yes

  If **yes**, identify the forms.

Form Number	Form Name
Form 940	Employer's Annual Federal Unemployment (FUTA) Tax Return
Form 941	Employer's Quarterly Federal Tax Return
Form 944	Employer's Annual Federal Tax Return
Form 1120	U.S. Corporation Income Tax Return
Form 1040	U.S. Individual Income Tax Return
Form 1041	U.S. Income Tax Return for Estates and Trusts
Form 1065	U.S. Return of Partnership Income
Form 1065-B	U.S. Return of Income for Electing Large Partnerships
Form 2350	Application for Extension of Time to File U.S. Income Tax Return
Form 4868	Application for Automatic Extension of Time to File U.S. Individual Income Tax Return
Form 9465	Installment Agreement Request
Form 8453	U.S. Individual Income Tax Transmittal for an IRS e-File Return

  11.f. Does the system receive SBU/PII from **Employee** forms (such as the I-9)?   No

F. DISSEMINATION OF PII

12. Does this system disseminate SBU/PII?   Yes

  12.a. Does this system disseminate SBU/PII to other IRS Systems?   Yes

  If **yes**, identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name	Current PCLIA	Approval Date	SA&A?	Authorization Date
Modernized Tax Return Database	Yes	11/06/2015	No	
Integrated Data Retrieval System	Yes	08/29/2017	Yes	12/21/2016

  Identify the authority.   Title 26 United States Code (USC) Internal Revenue Code (IRC) National Institute of Standards and Technology (NIST)Special Publication 800-122 NIST Special Publication. 800-122, 59 pages (Apr. 2010)
  For what purpose?   Tax administration and taxpayer service support IRS employees working active tax cases within each business function across the entire IRS. allowing IRS employees to take specific actions on taxpayer account issues, track status and post transaction updates back to the master files.

  12.b. Does this system disseminate SBU/PII to other Federal agencies?   Yes

If **yes** identify the full names of the federal agency(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) / Memorandum of Understanding (MOU).

Organization Name	Transmission method	ISA/MOU
United States Department of Agriculture	File is picked up via the Tumbleweed Secure Data Transfer (SDT). Tumbleweed has an integrated web server based off of Apache that utilizes Hypertext Transfer Protocol Secure with Advanced Encryption Standard Encryption. SDT is used to provide files to external IRS customers.	Yes

Identify the authority.   IRC Section 6103, 31 USC 1535/Federal Acquisition Regulation (FAR) 17.5, IRS computes Adjusted Gross Income (AGI) data and passes it to United Stated Department of Agriculture (USDA) assisting them in determining Federal Farm Program payment eligibility.

Identify the routine use in the applicable SORN (or Privacy Act exception).   Internal and external stakeholders need access to the PII data fields since these fields identify the taxpayer.

For what purpose?   IRC Section 6103, 31 USC 1535/FAR 17.5, IRS computes AGI data and passes it to USDA assisting them in determining Federal Farm Program payment eligibility.

12.c. Does this system disseminate SBU/PII to State and local agencies?   No

12.d. Does this system disseminate SBU/PII to IRS or Treasury contractors?   No

12.e. Does this system disseminate SBU/PII to other Sources?   No

G. PRIVACY SENSITIVE TECHNOLOGY

13. Does this system use social media channels?   No

14. Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, Radio Frequency Identification (RFID), etc.?   No

15. Does the system use cloud computing?   No

16. Does this system/application interact with the public?   No

H. INDIVIDUAL NOTICE AND CONSENT

17. Was (or is) notice provided to the individual prior to collection of information?   Yes

17.a. If **yes**, how is notice provided? Was the individual notified about the authority to collect the information, whether such is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects, if any, if they decide not to provide any of the requested information?
Notice is provided to individuals by other IRS applications or through forms (e.g., 1040 forms) that interact directly with the taxpayer at the time of collection. Due process is provided pursuant to Title 5 USC.

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

    18.a. If **yes**, describe the mechanism by which individuals indicate their consent choice(s):
This system does not collect any information directly from taxpayers. All information that is stored in this system comes from the submission of tax returns submitted directly to the IRS through other IRS systems. Information from the tax returns is subsequently shared from the other applications to this system. The tax return form provides taxpayers information regarding the opportunity to decline or consent to providing the information.

19. How does the system or business process ensure due process regarding information access, correction and redress?
This system is only a repository of taxpayer information submitted directly to the IRS through other IRS applications. This system does not interact with taxpayers directly and thus "due process" is addressed by other IRS applications that directly interact with taxpayers. Any issues that are identified by these other means will submit changes to this system through automated methods so an auditable record may be maintained. Due process is provided pursuant to 5 USC.

I. INFORMATION PROTECTION

20. 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

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

    IRS Employees?   Yes

IRS Employees?	Yes/No	Access Level (Read Only/Read Write/ Administrator)
Users	Yes	Read-Only
Managers	Yes	Read-Only
Sys. Administrators	Yes	Read and Write
Developers	No	

    Contractor Employees?   No

    21.a. How is access to SBU/PII determined and by whom? Employees request access to TRDB by submitting an Online (OL) 5081 which must be approved by their manager. When an employee is terminated or transferred from the IRS, their manager submits an OL5081 request to remove their access to the system.

I.1 RECORDS RETENTION SCHEDULE

22. 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

    22.a. 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.

TRDB is a recordkeeping repository for transcribed corporate return data and has a 50-year data retention requirement in concert with associated returns. The Records Office and TRDB system owners will work together to validate and potentially update TRDB dispositions to accurately fit data collection activities and maintenance needs. All records housed in the TRDB system will be erased or purged from the system in accordance with approved retention periods. It is the official repository for data and documents and has National Archives and Records Administration approval to affect data disposition. Any records generated and maintained by the system will be managed according to requirements under IRM 1.15.1 and 1.15.6, and will be destroyed using IRS Records Control Schedule 29, Item 445 and as coordinated with the IRS Records and Information Management Program and IRS Records Officer.

I.2 SA&A OR ASCA

23. Has the system been through Security Assessment and Authorization (SA&A) or Annual Security Control Assessment (ASCA)?   No

    23.c. If **no**, is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements?   Yes

23.1. Describe in detail the system's audit trail.   TRDB has a Cybersecurity approved audit plan. TRDB's audit log shows failed logon attempts because either the user account-name or password is incorrect. Audit events that are application-specific are recorded in an audit trail log, transaction log and error log. Application-level audit trails monitor and log end-user activities (including administrative users). Event records specify data files opened and closed, specific actions, such as reading, editing, deleting records or fields, and printing reports, etc. A full audit plan is available in DocIT (web-based electronic document management system).

J. PRIVACY TESTING

24. Does the system require a System Test Plan?   Yes

    24.a. If **yes**, If yes, was the test plan completed?   Yes

        24.a.1. If **yes**, where are test results stored (or documentation that validation has occurred confirming that requirements have been met)?   They are stored in DOCIT in this folder: Cabinets/Corporate Data/TRDB (Tax Returns Database)/TRDB FS2019/05 - Debug & Test/05.2-Project Level Test/Unit Test/Retrieve Team

        24.a.2. If **yes**, were all the Privacy Requirements successfully tested?   Yes

        24.a.3. If **yes**, are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved?   No

24.1. Describe what testing and validation activities which have been conducted or are in process to verify and validate that the applicable Privacy Requirements (listed in header) have been met?   TRDB is a non-Federal Information Security Management Act reportable system. It relies on NIST controls from the parent information system -- IBM Master File/IAP/CAPS Platform (GSS-21). Tests and validation activities are conducted on GSS-21 management, technical and operational controls to verify and validate that the applicable privacy requirements have been met.

K. SBU Data Use

25. Does this system use, or plan to use SBU Data in Testing?   No

L. NUMBER AND CATEGORY OF PII RECORDS

26. Identify the number of individual records in the system for each category:

          26.a. IRS Employees: 50,000 to 100,000
          26.b. Contractors: Not Applicable
          26.c. Members of the Public: More than 1,000,000
          26.d. Other: No

M. CIVIL LIBERTIES

27. Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment?   No

28. Is the system information used to conduct data-mining as defined in the *Implementing the Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?*   No

29. Will this system have the capability to identify, locate, and monitor individuals or groups of people?   No

30. Does Computer matching occur?   No

N. ACCOUNTING OF DISCLOSURES

31. 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

    31.a. 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

    31.b. If **no**, accounting of Disclosures risk noted. Contact Disclosure to develop accounting of disclosures. Explain steps taken to develop accounting of disclosures process.

    31.c. If **N/A**, explain the Exemption and/or Disclosure s response.

End of Report