NOTE: The following reflects the information entered in the PIAMS website.

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: 4/24/15 PIA ID Number: **1337**

1. What type of system is this? Corporate Data Initiative, CDI

2. Is this a new system? No

2a. If **no**, is there a PIA for this system? Yes

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

Corporate Data Initiative, CDI, MS3/4b

Next, enter the **date** of the most recent PIA. 5/30/2013 12:00:00 AM

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

No	Addition of PII
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

Were there other system changes not listed above? Yes

If yes, explain what changes were made. This PIA is due to the expiration of the prior PIA which isn't a choice above. The system has not changed, however the previous PIA did mention FRP (sub application) which was not converted therefore changes were made to the system description to remove any reference to FRP.

3. Check the current ELC (Enterprise Life Cycle) 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
No	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? Yes

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.

Corporate Data Initiative (CDI) will address the business need to have a relational database management system (RDBMS) that will be centrally located, secure, and meet enterprise standards. CDI will reduce costs by providing one security SA&A, provide for continuity and simplify maintenance. CDI will also offer the ability to quickly meet business needs when new compliance databases are required to meet business goals. CDI currently has two applications that are housed within the CDI SQL Server back end (not part of the SharePoint hardware and database farm). They are Tax Equity & Fiscal Responsibility Act (TEFRA) and Transmittal Database. All users with approved access to the subsystems will access through SharePoint 2010 as the front-end general user interface (GUI). SharePoint will provide application access based on the Active Directory group the user is permissioned. The user is required to submit an OL5081 to request access to the application based on their user role. After management approval, the Active Directory maintenance SA adds the user's SEID to the appropriate Active Directory group specific to each application. The Active Directory groups are added to SharePoint groups that control the user's access to the application and data. SharePoint will only display the site menus and underlying data the users are authorized to access. Users will not be able to view/access site menus or data they are not granted access. Once migrated, the application will be considered a subsystem to the overarching CDI umbrella program. Data content for each subsystem is isolated from the other. Every time a new application is migrated, CDI will setup a separate database in the single-instance multi-tenant architecture of MS SQL Server. All the data available on the subsystem portion of the site is stored within the respective subsystem SQL Server database instance. This SQL server is not part of the SharePoint infrastructure. PII data is not stored on the SharePoint. All data is saved on the CDI SQL server.

B. PII DETAIL

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

6a. If **yes**, does the system use, collect, receive, display, store, maintain, or disseminate Social Security Numbers (SSN s) or variations of SSN s (i.e. last 4 digits, etc.)? Yes

If **yes**, check who the SSN (or SSN variation) is collected on.

Yes	On Primary	Yes	On Spouse	No	On Dependent

If **yes**, check all types SSN s (or variations of SSN s) that apply to this system:

Yes	Social Security Number (SSN)
Yes	Employer Identification Number (EIN)
Yes	Individual Taxpayer Identification Number (ITIN)
No	Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
No	Preparer Taxpayer Identification Number (PTIN)

Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN s (or variations of SSN s).

No mitigation strategy is feasible. The provided data is required in order to have sufficient and accurate data to replicate what taxpayers file.

6b. Does this system contain other (non-SSN) PII that it uses, collects, receives, displays, stores, maintains, or disseminates according to Privacy Requirements? (i.e. Names, addresses, etc.) Yes

If **yes**, specify the information.

No PII Elements found.

6c. Does this system contain SBU information the system that it uses, collects, receives, displays, stores, maintains, or disseminates? No

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

6e. 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

6f. 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 variations) are used, explicitly explain why use of SSNs meets this criteria. Be specific.

The collection of PII in this system is needed for tax administration. The applications within CDI are used for the monitoring and processing of tax examinations.

8. How is the SBU/PII verified for accuracy, timeliness, and completeness? Explain how steps are taken to ensure that all information maintained by the system that is used by IRS to make any adverse determination about an individual's rights, benefits, and/or privileges is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination.

The taxpayer related data is entered into the system from the tax return by the tax examiner. As the case is processed, the accuracy of the data is reviewed and verified by each person in the workflow. This ensures data entered by the original creator is reviewed and updated if needed.

C. PRIVACY ACT AND SYSTEM OF RECORDS

9. Are 10 or more records containing SBU/PII maintained, stored, and/or transmitted by or through this system? Yes

9a. If **yes**, are records in the system retrieved by any personal identifier (e.g., name, SSN, Photograph, IP Address) for an individual? Yes

If **yes**, is there a System of Records Notice(s) or SORNs that addresses the PII records in this system? Yes

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

No SORN Records found.

If **yes**, does the System of Records Notice(s) (SORN) published in the Federal Register adequately describe the records as required by the Privacy Act? Yes

D. RESPONSIBLE PARTIES

10. Identify the individuals for the following system roles.

N/A

E. INCOMING PII INTERFACES

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

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

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

System Name	Current PIA?	PIA Approval Date	SA & A?	Authorization Date
AIMS-R subsystem: Partnership Control System	Yes	07/02/2014	No	

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

11c. Does the system receive SBU/PII from State or local agency (-ies)? No

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

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

If **yes**, identify the forms

Form Number	Form Name
1040	US Individual Income Tax Return
1120	US Corporation Income Tax Return
1120S	US Income Tax for an S Corporation
1065	US Return of Partnership Income

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

F. PII SENT TO EXTERNAL ORGANIZATIONS

12. Does this system disseminate SBU/PII? 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, cloud, global position system (GPS), biometrics, 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/is notice provided to the individual prior to collection of information? Yes

17a. 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?
The system uses data entered from tax returns filed by taxpayers. They are notified of such collection by the Privacy Act Notice in the tax return instructions.

18. Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information? No

Tax returns filed by taxpayers are the source of data input into the system.

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

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 and Write
Managers	Yes	Read and Write
Sys. Administrators	Yes	Administrator
Developers	Yes	Administrator

Contractor Employees? Yes

Contractor Employees?	Yes/No	Access Level	Background Invest.
Contractor Users	No		
Contractor Managers	No		
Contractor Sys. Admin.	No		
Contractor Developers	Yes	Administrator	Moderate

21a. How is access to SBU/PII determined and by whom? Access to all information on the system is restricted via Role Base Access Control and through integration with OL5081 for user creation. Only those authorized to view the data will have access to the information. The employee will initiate the OL5081 request. The applications OL5081 has different selections based on the level of access to be granted to the requesting user. This is approved by the employee's manager. Approval must be granted by the user's manager, the Technical POC, and the Enterprise LAN Account Administration Group, before the account is created and the access level granted. Upon termination or when a user no longer needs access to the IRS systems or applications, the user's manager or designated official, completes OL5081 requesting termination of access for the user.

21b. If computer matching occurs, can the business owner certify that it meets requirements of IRM 11.3.39 Disclosure of Official Information, Computer Matching & Privacy Protection Act?

Not Applicable

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? No

If **no**, how long are you proposing to retain the records? Please note, if you answered no, you must contact the IRS Records and Information Management Program to initiate records retention scheduling before you dispose of any records in this system.

CDI is non-recordkeeping. It is a project that addresses the business security and infrastructure needs of small databases. Records created and/or maintained in those systems will be scheduled in the context of those systems and documented/published in the Internal Revenue Service IRMs 1.15, exact Records Control Schedules and item numbers to be determined. SB/SE and the IRS Records and Information Management (RIM) Program Office will work together to address CDI-related scheduling needs.

I.2 SA&A OR ECM-R

23. Has the system been through SA&A (Security Assessment and Authorization) or ECM-R (Enterprise Continuous Monitoring Reauthorization)? Yes

23a. If **yes**, what date was it completed? 4/6/2015 12:00:00 AM

23.1 Describe in detail the system s audit trail. The applications have application files, data files, and application-specific logs that reside on a Windows application server. The application uses an SQL database. Audit events that are application-specific are recorded in audit trail logs. The application has audit logs that are located on the Windows server. Application audit logs are kept on the server for at least 90 days. Since the application has a security categorization of moderate, actions taken that add records to the database or update key information on records are recorded in the application audit logs. The applications are in the ESAT queue.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? No

24c. If **no**, please explain why. CDI was classified as COTS-Small other project for ELC. COTS-Small other projects are excluded from the for system test plan process. However, each application is tested and there is a system test plan and test cases for each sub application.

K. LIVE DATA TESTING

25. Does this system use, or plan to use Live Data in Testing? Yes

25a. If **yes,** was permission granted per the requirements of Form 13471 Live Data Request? Yes

If **yes,** provide the date the permission was granted. 10/23/2014 12:00:00 AM

.

25b. **If yes**, was testing performed in conformance with IRM 10.8.8 IT Security, Live Data Protection Policy? Yes

L. NUMBER AND CATEGORY OF PII RECORDS

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

26a. IRS Employees: Not Applicable
26b. Contractors: Not Applicable
26c. Members of the Public: 100,000 to 1,000,000
26d. 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 9/11 Commission Recommendations 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

N. ACCOUNTING OF DISCLOSURES

30. Does the system include or require disclosure of tax or employee information to anyone other than IRS employees or IRS contractors 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

End of Report