

---

**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 Submission: Apr. 27, 2012

PIA ID Number: **190**

---

**1. What type of system is this?** New, Non–Major System

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

---

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

Corporate Data Initiative, CDI

---

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

If yes, please state the previous system name, acronym, and release/milestone (if appropriate):

---

**3. Identify how many individuals the system contains information on**

Number of Employees: Under 50,000

Number of Contractors: Not Applicable

Members of the Public: Under 100,000

---

**4. Responsible Parties:**

---

N/A

---

**5. General Business Purpose of System**

---

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 or spreadsheets are required to meet business goals. CDI currently has three applications that are projected to migrate and will be housed within the CDI SQL Server back end. They are Tax Equity & Fiscal Responsibility Act (TEFRA), Frivolous Return Program (FRP), and Transmittal Database. All users who need access to the subsystems under the CDI umbrella program will access through SharePoint. SharePoint will provide site collection portal access based on the operating unit in which the subsystem falls under. Each operating unit is a site collection portal. CDI Campus Compliance Services (CCS) is an example of a site collection portal. The three subsystems currently targeted for migration are under the CDI Campus Compliance Services. Beside CCS, CDI is planning on providing this service to all of the other operating units under SB/SE, to include is Strategy & Finance, Communications & Stakeholder Outreach, Fraud/BSA, Enterprise Collection Strategy, Field Collection, Examination, Research, Specialty, and Smart HCO. The goal is to have this capability roll out enterprise wide in future iterations of the system. Once the users enter the SharePoint URL, the users may have access to multiple CDI subsystems' sub sites under each respective site collection portal, depending on their users' role. Each site collection portal will have a different URL. SharePoint will only display the operating unit site collection portals sub sites under which the users are authorized for access. Users will not be able to view/access site collection portals to which they are not granted access. A new dedicated sub site is created for each application that migrates over to the CDI umbrella program. Once migrated, the application will be considered a subsystem to the overarching CDI program. Data content for each subsystem is isolated from the other. Every time a new SharePoint sub site is created, 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.

**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:** 03/26/2012

---

**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 Yes

---

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

–Update the system description –Update the SORN. –Add in AIMS for the source of interconnection.

---

**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****8a. If No, what types of information does the system collect, display, store, maintain or disseminate?****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 Yes

Other No

*Other Source:* \_\_\_\_\_

---

**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	Yes	Yes	Yes
Social Security Number (SSN)	Yes	Yes	No
Tax Payer ID Number (TIN)	Yes	Yes	No
Address	Yes	Yes	Yes
Date of Birth	No	No	No

**Additional Types of PII:** No

No Other PII Records found.

---

**10a. Briefly describe the PII available in the system referred to in question 10 above.**

The system contains taxpayer data and it will also contain information about the employees that use the system. The employee data is used to complete letters and daily time records. The employee data includes SEID, IDRS number, office address and phone number.

**If you answered Yes to Social Security Number (SSN) in question 10, answer 10b, 10c, and 10d.**

---

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

26 USC 6109 requires inclusion of identifying numbers in returns, statements, or other documents for securing proper identification of persons required to make such returns, statements, or documents.

---

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

None

---

---

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

A mitigation strategy is currently not required.

**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.**

This is a new system and the full audit requirements have not been fully developed. The standard requirements for audit trails and logging will be implemented.

**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:

<u>System Name</u>	<u>Current PIA?</u>	<u>PIA Approval Date</u>	<u>SA &amp; A?</u>	<u>Authorization Date</u>
AIMS-R subsystem: Partnership Control System	Yes	08/29/2011	Yes	02/08/2012

b. Other federal agency or agencies: No  
If Yes, please list the agency (or agencies) below:

c. State and local agency or agencies: No  
If Yes, please list the agency (or agencies) below:

d. Third party sources: No  
If yes, the third party sources that were used are:

e. Taxpayers (such as the 1040): Yes

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

g. Other: No If Yes, specify:

---

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

---

**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 Yes  
To provide taxpayer services No  
To collect demographic data No  
For employee purposes No

Other: No

*If other, what is the use?*

---

**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

15a. If yes, with whom will the information be shared? The specific parties are listed below:

	Yes/No	Who?	ISA OR MOU**?
Other federal agency (-ies)			
State and local agency (-ies)			
Third party sources			
Other:			

\*\* Inter-agency agreement (ISA) or Memorandum of Understanding (MOU)

16. Does this system host a website for purposes of interacting with the public? No

17. Does the website use any means to track visitors' activity on the Internet?

If yes, please indicate means:

	YES/NO	AUTHORITY
Persistent Cookies	_____	_____
Web Beacons	_____	_____
Session Cookies	_____	_____
Other:	_____	_____ <i>If other, specify:</i>

---

**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? No

18a. If Yes, how is their permission granted?

---

19. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action? Not Applicable

19a. If Yes, how does the system ensure "due process"?

20. Did any of the PII provided to this system originate from any IRS issued forms? Yes

20a. If Yes, please provide the corresponding form(s) number and name of the form.

<u>Form Number</u>	<u>Form Name</u>
1040	Income tax form
1120S	S-Corp return
1120	Corporate return
1065	Partnership return

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

Written consent \_\_\_\_\_

Website Opt In or Out option \_\_\_\_\_

Published System of Records Notice in the Federal Register \_\_\_\_\_

Other: \_\_\_\_\_

**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

**21a. If Contractor operated, has the business unit provided appropriate notification to execute the annual security review of the contractors, when required?**

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

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

**If you answered yes to contractors, please answer 22a. (All contractor/contractor employees must hold at minimum, a "Moderate Risk" Background Investigation if they have access to IRS owned SBU/PII data.)**

**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?**

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

Access to the system will be governed by the OL5081 process and the various approval levels.

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

CDI will have has input validation processes that check character length, types, and formats to ensure data will be processed accurately.

**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?** No

**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.**

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.

---

**26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.**

The CDI application relies on or inherits from the MITS-21 and MITS-1 GSSs technical controls that secure data at rest, during transit, and protects from outside influences. Media protection controls are inherited from the IRS facilities that house the information system. Administrative policies and procedures have been developed to define the requirements for protection of data during transit, at rest, and in flight.

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

This is a new system and will follow all appropriate administrative and technical controls as outlined by database security requirements.

---

**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.**

The CDI application does not have any system monitoring or evaluation capabilities. CDI relies on MITS-1 to provide system monitoring and evaluation.

---

**29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 – IT Security, Live Data Protection Policy? Yes**

---

**29a. Has approval been received from the Office of Privacy Compliance to use Live Data in testing (if appropriate)?**

**29b. If you have received permission from the Office of Privacy Compliance to use Live Data, when was the approval granted?**

---

**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.**

<u>SORNS Number</u>	<u>SORNS Name</u>
TREAS/IRS 24.030	Customer Account Data Engine Individual Master File
TREAS/IRS 24.046	Customer Account Data Engine Business Master File
TREAS/IRS 34.037	IRS Audit Trail & Security Records System
TREAS/IRS 42.001	Examination Administrative File
TREAS/IRS 42.021	Compliance Programs and Project Files

**Comments**

---

**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)	<u>No</u>
Provided viable alternatives to the use of PII within the system	<u>No</u>
New privacy measures have been considered/implemented	<u>No</u>
Other:	<u>No</u>

**32a. If Yes to any of the above, please describe:**

NA

[View other PIAs on IRS.gov](#)