
A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Compliance Data Environment Release 3, CDEr3

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, PIA ID Number and milestone of the most recent PIA.

Compliance Data Environment, Release 3 , CDEr3, PIA ID Number: 408

Next, enter the **date** of the most recent PIA. 3/25/2013

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? No

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.

Compliance Data Environment, Release 3 (CDER3) eliminates the manual handling of paper tax returns and provides central and local monitoring of all aspects of the Audit classification process. The purpose of CDER3 is to automate and increase workload efficiencies and fairness of audit case selection, and to address alternative compliance treatment. CDER3 will automate current labor-intensive, manual analysis of data files not available in any other application, while incorporating fraud and collect ability indicators

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

6a. 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 who the SSN (or tax identification number) is collected on.

Yes On Primary Yes On Spouse Yes On Dependent

If **yes**, check all types SSN s (or tax identification numbers) 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)
Yes Practitioner Tax Identification Number (PTIN)

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 known mitigation strategy planned to eliminate the use of SSN for the system; SSN is required for the use of this system. The SSN number is needed to identify potential workload inventory.

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

If **yes**, specify the information.

<u>Selected</u>	<u>PII Element</u>	<u>On Primary</u>	<u>On Spouse</u>	<u>On Dependent</u>
Yes	Name	Yes	Yes	No
Yes	Mailing address	No	No	No
No	Phone Numbers	No	No	No
No	E-mail Address	No	No	No
Yes	Date of Birth	Yes	Yes	Yes
No	Place of Birth	No	No	No
No	SEID	No	No	No
No	Mother's Maiden Name	No	No	No
No	Protection Personal Identification Numbers (IP PIN)	No	No	No
No	Internet Protocol Address (IP Address)	No	No	No

No	Criminal History	No	No	No
No	Medical Information	No	No	No
No	Certificate or License Numbers	No	No	No
No	Vehicle Identifiers	No	No	No
No	Passport Number	No	No	No
No	Alien (A-) Number	No	No	No
No	Financial Account Numbers	No	No	No
No	Photographic Identifiers	No	No	No
No	Biometric Identifiers	No	No	No
No	Employment (HR) Information	No	No	No
Yes	Tax Account Information	Yes	No	No

6c. 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

<u>Selected</u>	<u>SBU Name</u>	<u>SBU Description</u>
Yes	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.
No	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
No	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
No	Criminal Investigation Information	Information concerning IRS criminal investigations or the agents conducting the investigations.

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)

<u>No</u>	PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)
<u>Yes</u>	SSN for tax returns and return information is Internal Revenue Code Section 6109
<u>No</u>	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 tax identification numbers) are used, explicitly explain why use of SSNs meets this criteria. Be specific.

CDEr3 receives tax return information from the Compliance Data Environment (CDE) application. This tax return data originally comes from the tax return form 1040 series. Data elements from the 1040 taxpayer return form include date of birth, name, address, gross income, TINs, audit history, deductions, and DIF score. CDEr3 receives data from CDE, which validates the data prior to sending it to the CDEr3 database. Thus, this taxpayer return data comes from an authoritative source and cannot be changed (authoritative source in this case is CDE; pulling the data directly from the Masterfile. This data can't be changed as it is loaded). The RBE filters this data, but does not actually change any of the taxpayer data and variables. No outside contractors will have access to the system in the production environment.

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

CDEr3 receives data from CDE, which validates the data prior to sending it to the CDEr3 database. Thus, this taxpayer return data comes from an authoritative source and cannot be changed (authoritative source in this case is CDE; pulling the data directly from the Masterfile. This data can't be changed as it is loaded). The RBE filters this data, but does not actually change any of the taxpayer data and variables.

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.

SORNS Number SORNS Name

Treas/IRS 42.001 exam administrative files

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.

<u>System Name</u>	<u>Current PIA?</u>	<u>PIA Approval Date</u>	<u>SA & A?</u>	<u>Authorization Date</u>
Compliance Data Environment	Yes	04/10/2013	Yes	05/07/2010

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? Yes

If **yes**, identify the source that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

<u>Organization Name</u>	<u>Transmission method</u>	<u>ISA/MOU</u>
U.S. Census Bureau Allowable Living Expense (ALE) MS Access Database		No

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

If **yes**, identify the forms

<u>Form Number</u>	<u>Form Name</u>
1040	Individual Income Tax Return

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? Yes

12a. 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.

<u>System Name</u>	<u>Current PIA?</u>	<u>PIA Approval Date</u>	<u>SA & A?</u>	<u>Authorization Date</u>
SAP Business Objects	Yes	04/05/2013	Yes	04/05/2013

Identify the authority and for what purpose? SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns. Additional information can be found at these two links: <http://www.irs.gov/pub/irs-wd/00-0075.pdf> <http://www.law.cornell.edu/uscode/text/26/6109>

12b . Does this system disseminate SBU/PII to other Federal agencies? No

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

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

12e. 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, 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? No

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?

17b. If **no**, why not? If information is not collected directly from an individual, please discuss the factors considered in deciding to collect information from third party sources. CDER3 receives tax return information from the Compliance Data Environment (CDE) application. This tax return data originally comes from the tax return form 1040 series. Data elements from the 1040 taxpayer return form include date of birth, name, address, gross income, TINs, audit history, deductions, and DIF score. CDER3 receives data from CDE, which validates the data prior to sending it to the CDER3 database. Thus, this taxpayer return data comes from an authoritative source and cannot be changed (authoritative source in this case is CDE; pulling the data directly from the Masterfile. This data can't be changed as it is loaded). The RBE filters this data, but does not actually change any of the taxpayer data and variables. No outside contractors will have access to the system in the production environment.

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

18b. If no, why not? The information within CDER3 comes from the Compliance Data Environment (CDE) application. This system and associated forms provide the Privacy Act Notice to individuals. CDE3r does not directly provide individuals the opportunity to decline from providing information and/or from consenting to particular uses of the information. Notice, consent and due process are provided in the CDE application and related tax forms instructions, and pursuant to 5 USC.

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

The information within CDER3 comes from the Compliance Data Environment (CDE) application. This system and associated forms provide the Privacy Act Notice to individuals. CDE3r does not directly provide individuals the opportunity to decline from providing information and/or from consenting to particular uses of the information. Notice, consent and due process are provided in the CDE application and related tax forms instructions, and 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	No	
Managers	No	
Sys. Administrators	Yes	Read-Only
Developers	Yes	Read And Write

Contractor Employees? No

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

21a. How is access to SBU/PII determined and by whom? Access to the CDER3 servers and data therein is requested by the employee using the OL5081 system. The manager approves/disapproves the OL5081 based on the employees' job responsibilities and need-to-know.

- 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
- 22b. 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.
- CDEr3 is non-recordkeeping. It is not the official repository for any data or documents, and does not require a NARA-approved records control schedule to affect data disposition. CDEr3 is a rules-based batch processing application that automates the checking of tax filing non-compliance. CDEr3 does not generate, alter or store official records. The authoritative source of tax return data for CDEr3 comes from Compliance Data Environment (CDE), and CDE data and associated records are scheduled under National Archives Job Nos. N1-58-08-15 and N1-58-10-10. CDEr3 filtered data is transferred to Business Objects for working non-compliance issues. This system may require scheduling and is something the Records Office will pursue separate from CDEr3. For performance issues and data source restrictions it may be necessary to temporarily cache data in CDEr3. A script is needed to identify what is to be scrubbed after each successful data transfer, but a records control schedule for PTC is not required. Data retention requirements are defined in accordance with the recordkeeping systems from/to which the data is obtained/transferred. The method used for sanitization will follow NIST SP 800-88 guidelines.

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? 1/22/2016
- 23.1 Describe in detail the system s audit trail. CDEr3 does not have any end users to the application. Thus, there is no log-in to access the application. Audit trail information through CDEr3's database is controlled by Modernization & Information Technology Services (MITS)-30 Enterprise Operations Personnel (EOps). The CDEr3 database keeps audit trails for all files processed by the application, which reflect the file processed, data and time of processing, number of records (input/output), and any errors that occur from problems with the rules in the RBE, which have its own capabilities.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? No
- 24c. If **no**, please explain why. The CDEr3 program relies on Commercial-Off-The-Shelf (COTS) software called FICO Blaze Advisor and the IRS contracts the software licenses. System updates and changes to Blaze Advisor are performed by the FICO software company, not IRS employees or contractors.

K. SBU Data Use

25. Does this system use, or plan to use SBU Data in Testing? Yes
25a. If **yes**, was permission granted per the requirements of Form 14664, SBU Data Use Questionnaire or Form 14665, SBU Data Use Request?
Yes
If **yes**, provide the date the permission was granted. 12/9/2009
25b. If **yes**, was testing performed in conformance with IRM 10.8.8 Information Technology (IT) Security, Sensitive But Unclassified (SBU) Data 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: More than 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 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
