

Date of Approval: **March 19, 2019**

PIA ID Number: **3925**

SYSTEM DESCRIPTION

Enter the full name and acronym for the system, project, application and/or database.

Compliance Data Environment, CDE

Is this a new system?

No

Is there a PCLIA for this system?

Yes

What is the full name, acronym and milestone of the most recent PCLIA?

Compliance Data Environment, CDE, ID1685

What is the approval date of the most recent PCLIA?

3/23/2016

Changes that occurred to require this update:

Expiring PCLIA

Were there other system changes not listed above?

Yes

What were those changes?

Numerous code changes and minor enhancements

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

Enterprise Computing Center Configuration Control Board (ECC-CCB)

Current ELC (Enterprise Life Cycle) Milestones:

Operations & Maintenance (i.e. system is currently operational)

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

Yes

GENERAL BUSINESS PURPOSE

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.

The Compliance Data Environment (CDE) is a centralized, open-architecture automated information system which assists IRS employees in the identification, classification, and delivery of tax return information. CDE employees review tax returns and determine whether or not they are worthy of audit. Returns that are selected for audit are sent either electronically to the CDE Manager or to designated printers for delivery to the Exam group within SB/SE. CDE eliminates the manual handling of paper tax returns during the classification process and provides central and local monitoring of all aspects of the classification process. The classification process is performed by experienced Revenue Agents and Tax Compliance Officers. CDE replaced and consolidated several legacy systems across multiple platforms throughout the IRS, with a secure repository which allows authorized users to access taxpayer data from their IRS networked workstation. The application is composed of a Data Mart repository and a Workload Manager application server. The Workload Manager is the web-based Graphical User Interface (GUI) of CDE. The Workload Manager is the interface which CDE users utilize for the management of SB/SE tax record examination. The Data Mart stores all Individual Return Transaction Files (IRTF) and Business Return Transaction Files (BRTF) tax return data, in addition to selected master file fields from the 701 extracts for the four most recent tax years. Both Individual and Business Return Transaction Files include transcribed line items from taxpayer filed income tax returns. These files contain data such as taxpayer name and address, social security number (SSN), and information regarding dependents.

PII DETAILS

Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any other type of Sensitive but Unclassified (SBU) information or PII such as information about IRS employees or outside stakeholders?

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

What types of tax identification numbers (TIN) apply to this system?

Social Security Number (SSN)

List the approved Treasury uses of the SSN:

Legal/statutory basis (e.g. where collection is expressly required by statute)

When there is no reasonable alternative means for meeting business requirements

Explain why the authorized use(s) above support the new or continued use of SSNs (or tax identification numbers)

The SSN is needed in order to match K-1 documents and use the K-1 documents to match to business returns in order to improve the classification process.

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

The Office of Management and Budget memorandum M-17-12 requires that federal agencies develop a mitigation or elimination strategy for systems that use SSNs, which the Service continues to develop strategies to meet. An exception to that requirement is when the SSN is uniquely needed to identify a user's record. CDE requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer at this time. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns.

Employer Identification Number

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

Yes

Specify the PII Elements:

Name

Mailing address

Phone Numbers

Date of Birth

Standard Employee Identifier (SEID)

Financial Account Numbers

Employment Information

Tax Account Information

Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?

Yes

Specify the types of SBU from the SBU Types List

Proprietary data Business information that does not belong to the IRS

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

Are there other types of SBU/PII used in the system?

Yes

Describe the other types of SBU/PII that are applicable to this system.

Federal Tax Information - income amounts from tax returns; filing status; fact of filing; classification that a return has been selected for audit.

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

PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, & 6012e(a)

SSN for tax returns and return information is Internal Revenue Code Section 6109

Has the authority been verified with the system owner?

Yes

BUSINESS NEEDS AND ACCURACY

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.

Taxpayer information, to include name, SSN, and contact information is required to identify taxpayer's account. Additionally, taxpayer assets and personal property are required to ensure proper selection of returns for audit. Employee data maintained in the application is necessary to ensure only authorized users have access in and out of the application. Employee spousal information is maintained on the application to ensure adequate and legal privacy of personal information.

How is the SBU/PII verified for accuracy, timeliness and completion?

Several internal data validation processes have been implemented within the CDE application to ensure data input is accurate, complete, and valid. The application heavily relies on the User Interface Form Validation to perform validity, authenticity, and completeness checks. On the back end, the CDE application relies on CDE Request Message Validation to prevent script injection attacks through ASP.Net. These two methods of validation ensure that users are not allowed to enter malicious code. If malicious code is entered, Tivoli Monitoring will gather the error from the event log and will send an automatically generated email to the CDE. Regarding user input, format masks and syntax checks have been installed for most form fields to indicate for example, letters cannot be entered into a numeric data field, such as a phone number or date. Additionally, the application checks to ensure all required data fields are completed before a user can move to the next screen. Drop down menus are utilized throughout the application to minimize the amount of incorrect or invalid data entries. Prior to the release of data into the production environment, extensive testing is performed to verify the accuracy, timeliness and completeness of all data elements. The formal test process ensures that issues are addressed in the development environment (where initial testing takes place), then moved into the test environment (where extensive testing takes place), and finally pushed into production (where transfer process testing takes place). Transfer process testing examines the data that populates the database by ensuring all data is accurate. A record count validation process is also used to ensure information provided by separate systems or files is successfully loaded into the database. Data entering CDE from external sources is transmitted encrypted, primarily via the Enterprise File Transfer Utility (EFTU) transfer protocol to ensure data is not compromised during transfer. All incoming data is then routed through a BizTalk Server. XML received from external systems is checked against an XSD schema for validity. Non-XML data received from external systems is converted to XML via a BizTalk pipeline, map, and schema. This process also ensures that the non-XML data is in the proper format. Only after passing these schema validations are any CDE orchestrations or business objects invoked.

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.

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

Identify the Privacy Act SORN(s) that cover these records.

IRS 24.030 Customer Account Data Engine Individual Master File

IRS 24.046 Customer Account Data Engine Business Master File

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

Official Use Only

INCOMING PII INTERFACES

Does the system receive SBU/PII from other systems or agencies?

Yes

Does the system receive SBU/PII from IRS files and databases?

Yes

Enter the files and databases:

System Name: Security Audit and Analysis System (SAAS)

Current PCLIA: Yes

Approval Date: 4/13/2018

SA&A: Yes

ATO/IATO Date: 6/12/2017

System Name: IBM Mainframe (MITS-21 GSS)
Current PCLIA: Yes
Approval Date: 8/31/2018
SA&A: Yes
ATO/IATO Date: 9/17/2018

System Name: Integrated Data Retrieval System (IDRS)
Current PCLIA: Yes
Approval Date: 10/1/2018
SA&A: Yes
ATO/IATO Date: 10/14/2018

System Name: Financial Crimes Enforcement Network- WEBCBRS
Current PCLIA: Yes
Approval Date: 3/16/2016
SA&A: Yes
ATO/IATO Date: 5/19/2018

System Name: Audit Information Management System (AIMS-R)
Current PCLIA: Yes
Approval Date: 9/19/2018
SA&A: Yes
ATO/IATO Date: 8/22/2018

Does the system receive SBU/PII from other federal agency or agencies?

Yes

For each federal interface, identify the organization that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Name: Treasury Integrated Management Information System (TIMIS)
Transmission Method: Download from IRS Source
ISA/MOU: No

Does the system receive SBU/PII from State or local agency (-ies)?

No

Does the system receive SBU/PII from other sources?

No

Does the system receive SBU/PII from Taxpayer forms?

Yes

Please identify the form number and name:

Form Number: 1040 Form Name: U.S. Individual Income Tax Return

Form Number: 1040NR Form Name: U.S. Nonresident Alien Income Tax Return

Form Number: 1040PR Form Name: Planilla para la Declaración de la Contribución Federal sobre el Trabajo por Cuenta

Form Number: 1040SS Form Name: Form 1040-SS, U.S. Self-Employment Tax Return (Including the Additional Child Tax Credit for Bona Fi)

Form Number: 1120S Form Name: U.S. Income Tax Return for an S Corporation

Form Number: 1120 Form Name: U.S. Corporation Income Tax Return series

Form Number: 1065 Form Name: U.S. Return of Partnership Income

Form Number: 1041 Form Name: U.S. Income Tax Return for Estate and Trusts

Form Number: K-1 Form Name: Schedule K-1

Form Number: 1040EZ Form Name: U.S. Income Tax Return for Single and Joint Filers With No Dependents

Form Number: 1040A Form Name: U.S. Individual Income Tax Return

Form Number: 8610 Form Name: Annual Low-Income Housing Credit Agencies Report

Form Number: 8609 Form Name: Low-Income Housing Credit Allocation and Certification

Form Number: 8823 Form Name: Low-Income Housing Credit Agencies Report of Noncompliance or Building Disposition

Form Number: 8609-A Form Name: Annual Statement for Low-Income Housing Credit

Does the system receive SBU/PII from Employee forms (e.g. the I-9)?

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

Yes

Does this system disseminate SBU/PII to other IRS Systems?

Yes

Identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name: National Research Program (NRP)

Current PCLIA: Yes

Approval Date: 2/8/2017

SA&A: Yes

ATO/IATO Date: 3/1/2017

System Name: Integrated Production Mart (IPM)

Current PCLIA: Yes

Approval Date: 10/27/2017

SA&A: Yes

ATO/IATO Date: 4/1/2016

System Name: Return Review Program (RRP)

Current PCLIA: Yes

Approval Date: 10/6/2017

SA&A: Yes

ATO/IATO Date: 5/22/2018

Identify the authority

Office of Management and Budget (OMB) M 03-22 Internal Revenue Manual (IRM) 10.8.1

For what purpose?

We provide Value added fields (VAF) to IPM and RRP that are calculations on fields that they already receive such as Gross Profit and Net Profit percentage. This provides additional data for any type of selection or evaluative decisions. We provide prior 3 years data to NRP so that the current year returns selected have a history of the prior years returns. When evaluations are made of NRP returns selected, these prior 3 years are needed.

Does this system disseminate SBU/PII to other Federal agencies?

No

Does this system disseminate SBU/PII to State and local agencies?

No

Does this system disseminate SBU/PII to IRS or Treasury contractors?

No

Does this system disseminate SBU/PII to other Sources?

No

PRIVACY SENSITIVE TECHNOLOGY

Does this system use social media channels?

No

Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.?

No

Does the system use cloud computing?

No

Does this system/application interact with the public?

No

INDIVIDUAL NOTICE AND CONSENT

Was/is notice provided to the individual prior to collection of information?

Yes

How is notice provided? Was the individual notified about the authority to collect the information, whether disclosure is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects on the individual, if any, if they decide not to provide all or any of the requested information?

The information within CDE comes from various IRS Systems and forms. Those systems and forms provide the Privacy Act Notice to individuals. CDE 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 via the IRS systems and their related tax forms instructions, and pursuant to 5 USC.

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

No

Why not?

The IRS has the legal right to ask for information per IRC sections 6001, 6011, and 6012(a), and their regulations. The regulations state that "taxpayers must file a return or statement with IRS for any tax they are liable for". Their response is mandatory under these sections. The information within CDE comes from various IRS Systems and forms. Those systems and forms provide the Privacy Act Notice to individuals. CDE 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 via the IRS systems and their related tax forms instructions, and pursuant to 5 USC.

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

The information within CDE comes from various IRS Systems and forms. Those systems and forms provide the Privacy Act Notice to individuals. CDE 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 via the IRS systems and their related tax forms instructions, and pursuant to 5 USC.

INFORMATION PROTECTION

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

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

IRS Employees

Users: Read Only

Managers: Read Only

System Administrators: Administrator

Developers: Read Only

How is access to SBU/PII determined and by whom?

Specific Use role access is initiated by employee or manager through the Online 5081 process. Manager approval is required if access is initiated by employee. CDE User Administrators and Siteminder administrators approve specific user access by role into the CDE application. This CDE access is only given if job duties require access.

RECORDS RETENTION SCHEDULE

Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) approved a Records Control Schedule (RCS, IRS Document 12990) for the retention and destruction of official agency records stored in this system?

Yes

How long are the records required to be held under the corresponding GRS or RCS, and how are they disposed of? In your response, please provide the GRS or RCS chapter number, the specific item number, and records series title.

CDE data and associated records are scheduled under National Archives Job Nos. N1-58-08-15 and N1-58-10-10. Master files data is approved for destruction when 4 years old or when no longer needed for audit or operational purposes. CDE maintains the current tax year and the three preceding tax years of live data stored within the system. After each year has passed, data is then erased and eliminated from the system in the most appropriate method depending on the type of storage media used based upon documented IRS policies and procedures. CDE records disposition instructions will be published in IRS Document 12990, under Records Control Schedule 35 for Tax Administration Electronic Systems, Item 44 when next updated. Additionally, CDE application audit information is retained by the SAAS application for a minimum of seven years in compliance with IRM 10.8.3, Audit Logging Security Standards.

SA&A OR ASCA

Has the system been through SA&A (Security Assessment and Authorization) or ASCA (Annual Security Control Assessment)?

In-process

When is the anticipated date of the SA&A or ACS completion?

4/1/2019

Describe the system's audit trail.

A complete audit trail of the use of the system is captured and includes every login, logoff, file access and database query. The system monitors for security risks and compliance violations to ensure that the use of the system takes place only for an approved purpose that is within the professional responsibility of each user. CDE is following the appropriate audit trail elements pursuant to current Audit Logging Security Standards.

PRIVACY TESTING

Does the system require a System Test Plan?

Yes

Is the test plan completed?

Yes

Where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)?

SharePoint site Shared Documents\ CDE_Test_Documentation folder.

Were all the Privacy Requirements successfully tested?

Yes

Are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved?

No

Describe what testing and validation activities have been conducted or are in progress to verify and validate that the applicable Privacy Requirements (listed in header) have been met?

Compliance Data Environment (CDE) conducts continuous monitoring testing each year, with the eCM process. In addition, the SSP is reviewed annually during continuous monitoring initiatives, and updated at least every year or whenever there are significant changes to the system. An SSP was developed for the information system as part of the original eCM. This SSP has been maintained and updated as part of continuous monitoring and enterprise continuous monitoring (eCM) processes. As part of this eCM process, the SSP is being updated to ensure the security controls implemented for the system are accurately reflected, all applicable NIST SP 800-53 controls are addressed, and the document is compliant with NIST SP 800-18. As a part of the SA&A process, a SSP, PIA, IS

Contingency Plan (ISCP), Security Control Assessment (SCA) Plan, SCA Results Matrix and Security Assessment Report (SAR) were developed in accordance with NIST methodology.

SBU DATA USE

Does this system use, or plan to use SBU Data in Testing?

Yes

Was permission granted per the requirements of Form 14664, SBU Data Use Questionnaire or Form 14665, SBU Data Use Request?

Yes

Provide the date the permission was granted.

11/4/2015

Was testing performed in conformance with IRM 10.8.8 Information Technology (IT) Security, Sensitive But Unclassified (SBU) Data Policy?

Yes

NUMBER AND CATEGORY OF PII RECORDS

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

IRS Employees: 50,000 to 100,000

Contractors: More than 10,000

Members of the Public: More than 1,000,000

Other: No

CIVIL LIBERTIES

Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment?

No

Is the system information used to conduct 'data-mining' as defined in the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?

No

Will this system have the capability to identify, locate, and monitor individuals or groups of people?

No

Does computer matching occur?

No

ACCOUNTING OF DISCLOSURES

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