Date of Approval: March 23, 2016 PIA ID Number: **1685**

A. SYSTEM DESCRIPTION

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

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, CDE, ID320

Next, enter the **date** of the most recent PIA. 4/25/2013

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? Yes

If yes, explain what changes were made. Numerous code changes and minor enhancements.

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.

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.

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)
Yes 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).

None. TINs are needed to match documents from different sources.

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.

Selected	PII Element	On Primary	On Spouse	On Dependent

Yes	Name	Yes	Yes	No
Yes	Mailing address	No	No	No
Yes	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
Yes	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
Yes	Financial Account Numbers	No	No	No
No	Photographic Identifiers	No	No	No
No	Biometric Identifiers	No	No	No
Yes	Employment (HR) Information	No	No	No
Yes	Tax Account Information	Yes	Yes	No

6c. Does this system contain SBU information that is not PII, 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 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.

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

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.

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
Treasury/IRS 22.061	Information Return Master File
Treasury/IRS 24.030	CADE Individual Master File
Treasury/IRS 24.046	CADE Business Master File
Treasury/IRS 42.001	Exam Administrative Files
Treasury/IRS 34.037	IRS Audit Trail and Security Records System
Treas/IRS 42.021	Compliance Programs and Project 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. *Redacted Information For Official Use Only

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
Financial Crimes Enforcement Network (FinCEN)	Yes	02/05/2016	No	
Audit Information Management System (AIMS-R)	Yes	12/15/2015	No	
Security Audit and Analysis System (SAAS)	Yes	07/14/2015	No	
Negative TIN System (NTINS)	Yes	10/15/2015	No	
IBM Mainframe (MITS-21 GSS)	Yes	12/02/2014	No	
Enterprise Directory Authentication System (EDAS)	Yes	06/02/2014	No	
Integrated Data Retrieval System (IDRS)	Yes	08/03/2014	No	

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

If **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).

Organization Name	**Transmission method**	**ISA/MOU**
Treasury Integrated Management Information System (TIMIS).	From IRS source	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

Organization Name	**Transmission method**	**ISA/MOU**
Dun and Bradstreet	EFTU to SDT	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
1040NR	U.S. Nonresident Alien Income Tax Return
1040PR	Planilla para la Declaración de la Contribución Federal sobre el Trabajo por Cuenta
1040SS	Form 1040-SS, U.S. Self-Employment Tax Return (Including the Additional Child Tax Credit for Bona Fi
1120S	U.S. Income Tax Return for an S Corporation
1120	U.S. Corporation Income Tax Return series
1065	US Return of Partnership Income
1041	US Income Tax Return for Estate and Trusts
K-1	Schedule K-1
1040EZ	US Income Tax Return for Single and Joint Filers With No Dependents
1040A	U.S. 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? 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

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.
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.

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 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.

19. 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.

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	Administrator
Developers	Yes	Read-Only

Contractor Employees? No

21a. How is access to SBU/PII determined and by whom? Specific Use role access is initiated by employee or manager through the OL5081 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.

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? Yes

22a. 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.

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.

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? 1/26/2016

23.1 Describe in detail the system s audit trail. SAAS is a MITS owned, major application that stores audit logs from various IRS systems and provides on-line analytical processing of audit log data. The system allows the IRS and TIGTA to detect potential unauthorized accesses by CDE users and provides analysis capabilities and reporting for CDE managers. CDE records audit log records locally to an XML file, then sends a one way transmission of the records to SAAS once a day via EFTU. The following items are included in every Audit Trail record where applicable: Timestamp, UserID (SEID), Type of Event, Event ID, TAXFILERTIN, TAXPERIOD, MFT CODE, RETURNTYPE, TAX FILER TIN TYPE, SCRADDR, Role of User, Return Code, Session ID, and Vardata which is dependent upon the transaction in question.

J. PRIVACY TESTING

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

24b. If **yes**, Is the test plan in process or completed: Completed

24.3 If **completed/ or in process,** 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 years 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 be developed in accordance with NIST methodology.

24b.1. If **completed**, where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)? Results are stored in the Team Foundation Server (TFS) which resides on GSS-30.

24b.2. If **completed**, were all the Privacy Requirements successfully tested? Yes

24.2 If **completed**, are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved? No

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. 11/4/2015

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: 50,000 to 100,000
26b. Contractors: More than 10,000
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