Date of Approval: **April 21, 2023**

PIA ID Number: **7706**

SYSTEM DESCRIPTION

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

Corporate Data Initiative, CDI

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?

Corporate Data Initiative, CDI, 3317, O&M

What is the approval date of the most recent PCLIA?

3/23/2018

Changes that occurred to require this update:

Significant Merging with Another System

Expiring PCLIA

Were there other system changes not listed above?

Yes

What were those changes?

New component, Affordable Care Act Non-Filer was added to the CDI boundary.

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

SB/SE Technology Governance Board (TGB)

Current ELC (Enterprise Life Cycle) Milestones:

System Development/Milestone 4B

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.

Corporate Data Initiative (CDI) provides authoritative databases, refund identification, notice generation, and reporting. CDI is an umbrella that offers the ability to quickly meet business needs when new compliance databases are required to meet business goals. CDI currently has four applications under the umbrella. Two applications use SharePoint for the user interface and case data is saved in a Structured Query Language (SQL) database server assigned to CDI that is not part of the SharePoint database farm. The applications are Tax Equity & Fiscal Responsibility Act (TEFRA) and Transmittal. All users with approved access to the subsystems will access them through a SharePoint Online user interface. SharePoint will provide application access based on the Active Directory group the user is permissioned. The third and fourth applications are Employer Shared Responsibility Payment (ESRP) and Affordable Care Act Non-Filer (ACANF). ESRP and ACANF use a web-based user interface and data is saved in a SQL database server. All users with approved access to the subsystem will access through the web interface. User access will be validated by the system before access is granted.

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:

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 provided data is required in order to have sufficient and accurate data to replicate what taxpayers file. There is no alternative to the use of the social security number (SSN). The SSN is the significant part of the data being processed.

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

No mitigation strategy is feasible. The provided data is required in order to have sufficient and accurate data to replicate what taxpayers file. There is no alternative to the use of the social security number (SSN). The SSN is the significant part of the data being processed.

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
E-mail Address
Standard Employee Identifier (SEID)
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:

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.

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.

The cases are worked electronically and contain tax return data plus correspondence, tax calculations, case actions and electronic responses.

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.

The collection of PII in this system includes names, addresses, telephone numbers, and taxpayer identification numbers (SSNs, ITIN, etc.) and is needed for tax administration which includes examinations. The applications within CDI are used for the monitoring and processing of tax examinations under 6109.

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

The taxpayer related data is entered into the system from the tax return by the tax examiner (TEFRA/Transmittal) or imported from ACA Compliance Validation (ACV) using exported Business Objects reports. 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 or imported is reviewed and updated if needed.

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

IRS 34.037 Audit Trail and Security Records

IRS 42.001 Examination Administrative Files

IRS 42.021 Compliance Programs and Projects Files

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: ACA Compliance Validation
Current PCLIA: Yes
Approval Date: 5/19/1921
SA&A: No

System Name: AIMS-R
Current PCLIA: Yes
Approval Date: 3/14/2022
SA&A: Yes
ATO/IATO Date: 12/9/2022

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

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: 1120
Form Name: US Corporation Income Tax Return

Form Number: 1040
Form Name: US Individual Income Tax Return

Form Number: 1120S
Form Name: US Income Tax for an S Corporation

Form Number: 1065
Form Name: US Return of Partnership Income

Form Number: 1094-C
Form Name: Transmittal of Employer-Provided Health Insurance Offer and Coverage Information Returns

Form Number: 1095-C
Form Name: Employer-Provided Health Insurance Offer and Coverage Premium Tax Credit (PTC)

Form Number: 8962
Form Name: Premium Tax Credit (PTC)

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

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

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 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.

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

No

Why not?

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

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

The process and procedures are dictated by the Internal Revenue Manual guidelines. IRS policy allows individuals whose data is in the system the opportunity to clarify or dispute negative determinations through the appeals process. The Taxpayer Bill of Rights publication 1 outlines the baseline for 'due process' that business follows.

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 Write
Managers: Read Write
System Administrators: Administrator
Developers: Administrator

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 BEARS for user creation. Only those authorized to view the data will have access to the information. The employee will initiate the BEARS request. The applications BEARS entitlement has different selections based on the level of access to be granted to the requesting user which is approved by the employee's manager. Approval must be granted by the user's manager, the technical point of contact (POC), CDI approver and the Enterprise 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 BEARs request for termination of access for the user.

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?

No

You must work with the IRS Records and Information Management (RIM) Program Office to address records retention requirements before you dispose of any records in this system.

SA&A OR ASCA

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

Yes

What date was it completed?

2/17/2023

Describe 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 a 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.

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)?

The test results are stored on a SharePoint site.

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?

The test cases are completed to ensure a user cannot access the system if their SEID is not in the user table or is marked inactive in the user table. In addition, if the user has not accessed the application in 120 days, then their account is automatically marked inactive by the system and the user cannot access the system. The system does provide the user with a message explaining why access was denied.

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.

4/18/2023

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: Not Applicable

Contractors: Not Applicable

Members of the Public: 100,000 to 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