Date of Approval: **May 21, 2021**

PIA ID Number: **5957**

SYSTEM DESCRIPTION

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

Coverage Data Repository, CDR

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?

AFFORDABLE CARE ACT (ACA), COVERAGE DATA REPOSITORY (CDR)

What is the approval date of the most recent PCLIA?

5/3/2018

Changes that occurred to require this update:

Expiring PCLIA

Were there other system changes not listed above?

No

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

Data Delivery Services (DDS)

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?

No

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 Coverage Data Repository (CDR) maintains a centralized database for Exchange Periodic Data (EPD) and provides support to At-Filing Compliance Tax Processing of returns with Affordable Care Act (ACA) data and the following business capabilities: 1. CDR receives data from Integration Production Model (IPM) to support the ACA enrollment process. This data consists of last two years of tax return data, last three years of failure to reconcile data and Social Security Administration's (SSA) Data Master 1 (DM-1) data. It is requested from CDR by Income and Family Size Verification (IFSV) which in turn uses it to create a response to a Customer Service Management (CSM) request for taxpayer income information. 2. CDR receives Exchange Periodic Data (EPD) from the State's Insurance Exchanges. The State Insurance Exchanges consist of the web sites provided by states by which residents of those states can review and sign up for health insurance. A specific data set is created from this enrollment information and sent to the IRS (CDR) monthly. 3. CDR provides information to At-Filing Verification System (AVS). The At-Filing Verification system (AVS) obtains a file from CDR containing EPD data to compare information presented on a tax return to what has been provided in the EPD data. 4. CDR provides data to the Account Management System (AMS) system. A Customer Service Representative requests and receives data from CDR via the AMS system to help in reviewing a tax return or other taxpayer forms. There are several canned queries that can be run against CDR to populate AMS screens. 5. CDR provides EPD data to the IPM system. Since the IPM system is the IRS system of record for all data, CDR provides a copy of all EPD and Static Reference data for the current year to IPM monthly. 6. CDR receives a Unified Work Request (UWR) with Static Reference Data for the upcoming year. Static reference data contains information which is used to perform calculations specific to the ACA. This data changes, at most, yearly. CDR in turn provides this data to AMS and IPM. 7. CDR collects data and populates logs as required (performance, security, etc.). 8. CDR provides data to the Business Analytics (BA) system. CDR does not have an interface for online viewing or altering of individual data records. System administrator access to CDR is through two Commercial-Off-The-Shelf (COTS) products: Oracle (for supporting the repository itself) and Informatica (for supporting the CDR data load process). System administrators do not create, read, update or delete individual CDR data records as part of their normal responsibility. All data contained in CDR is maintained in its original state, with no change to the integrity or quality of the data. CDR does not manipulate or apply business rules to the data. Where taxpayer information is shared, all security and privacy requirements are adhered to and maintained by the Center for Medicaid/Medicare (CMS) Data Services Hub. Due process is provided pursuant to 26 United States Code (USC). There is no CDR interface for viewing or altering the records stored in any CDR schemas.

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)

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

Coverage Data Repository requires the use of SSNs 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.

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 Circular A-130 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. Coverage Data Repository 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
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.

Proprietary data   Business information that does not belong to the IRS.

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.

Date of Death Income Level

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.

CDR is responsible for receiving bulk data files from Integrated Production Model (IPM) and making the data within those files available to the Income and Family Size Verification (IFSV) application and other ACA consumer systems for use in administering the provisions of the ACA. Within those bulk data files are the SBU/PII data elements listed in this PIA. CDR does not have the ability to manipulate, change or delete any of the data elements contained within these files. Therefore, CDR does not itself have a business need or use for the SBU/PII identified in this PIA, other than to receive it from one application and store it for use by another application. This applies to all SBU/PII elements listed in this PIA. The SSN is used to provide tax return data to the Income and Family Size Verification process. The Taxpayer identification information and tax-related data is required per ACA regulations.

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

The data received from the IPM system is deemed reliable and the data is validated for accuracy by the contributing systems.

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

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: Integrated Production Model (IPM)
Current PCLIA: Yes
Approval Date: 6/6/2019
SA&A: Yes
ATO/IATO Date: 7/9/2018

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?

No

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: Information Sharing Reporting Analytics and Reporting (BDA-ISRANR)
Current PCLIA: Yes
Approval Date: 9/16/2019
SA&A: Yes
ATO/IATO Date: 1/1/2014

System Name: Compliance Data Warehouse (CDW)
Current PCLIA: Yes
Approval Date: 9/16/2020
SA&A: Yes
ATO/IATO Date: 4/15/2021

System Name: Information Sharing and Reporting Enterprise Service Bus (ISRS-ISRESB)
Current PCLIA: No
SA&A: Yes
ATO/IATO Date: 4/28/2021

System Name: Integrated Production Model (IPM)
Current PCLIA: Yes
Approval Date: 3/30/2016
SA&A: No

System Name: ACA Verification Service (AVS)
Current PCLIA: Yes
Approval Date: 11/20/2020
SA&A: Yes
ATO/IATO Date: 6/17/2021

Identify the authority.

IRC 6103(h)

For what purpose?

Information Sharing Reporting Analytics and Reporting (BDA-ISRANR) - Provides reporting capability on Exchange Periodic Data (EPD) captured in CDR and reported through Business Analytics (BA). Compliance Data Warehouse (CDW) - Provides EPD to CDW for APTC compliance and general statistical analyses. Information Sharing and Reporting Enterprise Service Bus (ISRS-ISRESB) - The ESB mediates the communication between IFSV requests and CDR responses (IFSV uses CDR data to determine applicant eligibility for the Advanced Premium Tax Credit for CMS). Integrated Production Model (IPM) - CDR provides EPD data to the IPM system. Since the IPM system is the IRS system of record for all data, CDR provides a copy of all EPD and Static Reference data for the current year to IPM monthly. ACA Verification Service (AVS) - The At-Filing Verification system (AVS) obtains a file from CDR containing EPD data to compare information presented on a Tax Return to what has been provided in the EPD data.

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 collection of tax information from individuals is provided for by the Federal Tax Regulation and provided to use by the Affordable Care Act processes by the Patient Protection and Affordable Care Act.

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

No

Why not?

Mandated by Federal Tax Regulations. The information is collected while carrying out the Internal Revenue laws of the United States; an individual cannot decline providing the information.

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

All data contained in CDR is maintained in its original state, with no change to the integrity or quality of the data. CDR does not manipulate or apply business rules to the data. All due process considerations for any system that uses data stored in CDR are the responsibility of that system.

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

> System Administrators: Read Write

IRS Contractor Employees

> Contractor System Administrators: Read Write

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

> Access to Coverage Data Repository is requested via an Online (OL) Form 5081. Access is granted on a need-to-know basis. The OL5081 enrollment process requires that an authorized manager approve access requests on a case by case basis. Access approval is based on the Users role(s) and responsibilities. Users are given the minimum set of privileges required to perform their regular and recurring work assignments; they are restricted from changing the boundaries of their access without management approval. The employee's access will be terminated once they no longer require access to the Database. Deletion from the active access role is also performed through the OL5081.

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?

4/16/2020

Describe the system's audit trail.

CDR does not have an interface for online viewing or altering of individual records. System administrators do not create, read, update or delete individual CDR data records as part of their normal responsibility. The CDR audit process and trail is to: - Identify actionable events for each CDR process or COTS product. These are events that either result in CDR data being created, read, updated or deleted, or that result in system administrators altering or affecting the CDR system environment. - For each actionable event, the appropriate auditable event is created that captures sufficient information to support later review or analysis of the event. The auditable event creates audit records that are first written to logs, using the capabilities provided by each COTS product or process. There is a large list of identified actionable and auditable events and they are documented in the Audit Plans of either the CDR application or its supporting COTS products. For example, database level auditing is being performed by IBM Guardium. IBM Guardium applies the Oracle audit plan to the data it captures and passes that data to ArcSight. (Note: Security Audit and Analysis System (SAAS) auditing requirements have been deferred by Enterprise Security Audit Trails (ESAT) Program Management Office to a later release).

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)?

DocIT

Were all the Privacy Requirements successfully tested?

No

Please explain which Privacy Requirements were not tested and why?

CDR is a machine-to-machine application that is not accessible to the public, thus limiting privacy issues. Privacy requirements were addressed during system design and are reviewed during each new PCLIA approval.

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?

Testing to ensure the functionality of the approved system changes for ACA CDR M&E, Milestone 4B (MS4B); the integrity of data exchanged between interfaces and the integration of the systems across the tax processing systems from a business perspective.

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.

11/16/2018

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: 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