Date of Approval: **April 18, 2023**

PIA ID Number: **7672**

SYSTEM DESCRIPTION

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

Common Data Processing Framework, CDPF

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?

4692, Common Data Processing Framework, CDPF

What is the approval date of the most recent PCLIA?

6/10/2020

Changes that occurred to require this update:

Significant System Management Changes

Expiring PCLIA

Were there other system changes not listed above?

Yes

What were those changes?

The Common Data Processing Framework (CDPF) security boundary was established to include the data distribution framework establishing a modern, Java-based platform on Linux operating system to distribute individual tax data to downstream systems and include CADE 2 Transition State 2 (TS 2) application functionality. The major design components (Data Services Framework (DSF), the Auto Rules Converter (ARC)) for this data distribution framework never went into production. The solution for data distribution is being redesigned for target state. All but 1 TS 2 applications went into production using Tier 2 servers, the Financial Recap Report (FRR) project. The Financial Recap Report (FRR) project has now been moved from the CDPF Security Authorization Boundary (SAB) into the Customer Account Data Engine (CADE) 2 SAB and run on the mainframe. The only remaining component within the CDPF boundary is the Capture Data Change (CDC) Tool.

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

Sustaining Operations (SO) ESC

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 Common Data Processing Framework (CDPF) is currently being redesigned however, the Capture Data Change (CDC) Tool remains in production and is used to populate data from the CADE 2 database to the Operational data Store (ODS). The CDPF security boundary was established to include the data distribution framework establishing a modern, Java-based platform on Linux operating system to distribute individual tax data to downstream systems and include CADE 2 Transition State 2 (TS 2) application functionality. The major design components (Data Services Framework (DSF), the Auto Rules Converter (ARC)) for this data distribution framework never went into production. The solution for data distribution is being redesigned for target state. All but 1 TS 2 applications went into production using Tier 2 servers, the Financial Recap Report (FRR) project. The Financial Recap Report (FRR) project has now been moved from the CDPF Security Authorization Boundary (SAB) into the Customer Account Data Engine (CADE) 2 SAB and run on the mainframe. The only remaining component within the CDPF boundary is the Capture Data Change (CDC) Tool.

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 SSN is the only unique identifier associated with taxpayers, spouses, and dependents that can be used to ensure the correct record is accessed. The CDC Tool disseminates a copy of the CADE 2 database to the Operational Data Store. This includes the SSN.

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

The CDC Tool only transport data from the CADE 2 database to the Operational Data Store. It is important that feeds continue to reach downstream legacy systems that do not have the ability to use SSN alternatives. Even though an alternative is not used immediately, the use of the SSN will continue to be assessed to determine when the SSN usage may be mitigated or eliminated. Until such time, the SSNs are used within this system in accordance with Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns.

Employer Identification Number

Other Taxpayer 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
Protection Personal Identification Numbers (IP PIN)
Financial Account Numbers
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:

Agency Sensitive Information - Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission.

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?

No

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 Personally Identifiable Information (PII) is initially collected from the IRS 1040 forms and all supplemental documentation by other applications in the pipeline, which is processed by IMF and recorded in the CADE 2 database. individual tax processing data from the CADE 2 database is replicated in the ODS for business reporting, using the CDC Tool. This includes the SSN, since it is the one unique identifier that can be used to link taxpayer accounts for account analysis and reporting.

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

The CDC tool does not process data it only synchronizes moves data from CADE 2 DB to CADE 2 Operational Data Store. between databases, Database balance and control reports are used to ensure accuracy and completeness. As tax return information is processed by the databases or other IRS systems fed by the databases, SBU/PII are verified for accuracy, timeliness, and completeness.

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

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: Customer Account Data Engine 2
Current PCLIA: Yes
Approval Date: 8/18/2021
SA&A: Yes
ATO/IATO Date: 3/16/2023

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: Integrated Production Model (IPM)
Current PCLIA: Yes
Approval Date: 10/26/2022
SA&A: Yes
ATO/IATO Date: 6/30/2022

Identify the authority.

The authority for processing taxpayer information is 5 U.S.C. 301 and 26 U.S.C. 7801.

For what purpose?

The purpose is for synchronizing tax return information between internal IRS systems in order for it to be processed and passed on to other downstream IRS businesses for further processing.

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?

Notice is provided to individuals by other IRS applications or through forms (e.g.,1040 forms) that interact directly with the taxpayer at the time of collection where Due Process is provided pursuant to 5 USC. The CDC Tool extracts data from existing CADE 2 database and is several systems removed from the data collection.

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

Yes

Describe the mechanism by which individuals indicate their consent choice(s):

No information used within the CDPF security boundary is collected directly from taxpayers. All information that is processed by CDPF comes from tax information collected through tax forms or other applications that interact with taxpayers. It is at the time of collection that individuals have the opportunity to decline or provide consent.

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

Due Process is provided 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

System Administrators: Administrator

IRS Contractor Employees

Contractor Developers: Read Write

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

All contractors and employees must go through the Public Trust Clearance process before access is considered. Once cleared, access to projects within the CDPF boundary is obtained through the Business Entitlement Access Request System (BEARS) process. All access must be approved via the BEARS system by the user's manager who reviews the access request at the time of submission and on an annual basis in order to verify the request and if the user has a need-to-know. The system administrators/approvers will also verify group membership to ensure system rights are limited based on the employee or contractor's need-to-know in order to perform their official duties. For non-production supporting environments users must complete the necessary SBU (live) data training, request access through BEARS, and in some cases as outlined by the requirements set forth within the IRM submit an elevated access letter that is approved by the Associate Chief Information Officer (ACIO) prior to granting access. The non-production environment will also routinely review access lists and verify accounts, removing ones that are no longer necessary. Every individual is reminded of their Unauthorized Access (UNAX) requirements where they are restricted to see certain taxpayer data and, in many instances, a third-party tool is implemented to restrict access to that data.

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?

3/20/2023

Describe the system's audit trail.

The SA&A controls are assessed annually in accordance with the Annual Security Control Assessment (ASCA) to ensure system security and privacy compliance. Vulnerability scans and policy checkers are routinely run. If a vulnerability is detected efforts are made to address the concern upon discovery The CDC Tool has an Audit Control Response (ACR) worksheet that it follows.

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)?

When data from a production environment is needed for development or testing in a non-production environment, IRM 10.5.8, Sensitive But Unclassified (SBU) Data Policy: Protecting SBU in Non-Production Environments, is followed.

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 overarching privacy requirements are defined in testable requirements that are reviewed by the development team. The identified requirements are then tested, and results documented. Any risks that are discovered are reviewed and addressed. All this is being coordinated by Requirements Engineering Program Office and Cybersecurity and tracked in the Rational Requirements Tool and developer security assessment testing.

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.

9/6/2022

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