Date of Approval: **March 23, 2023**

PIA ID Number: **7643**

SYSTEM DESCRIPTION

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

Enterprise Data Platform Release 2.2, EDP WC2

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?

Enterprise Data Platform EDP Workplace Community MS 4b, #7339

What is the approval date of the most recent PCLIA?

10/21/2022

Changes that occurred to require this update:

Addition of Personally Identifiable Information (PII)

Were there other system changes not listed above?

Yes

What were those changes?

EDP Workplace Cloud Community (WC2) platform will host multiple datasets, for Rel 2.2 - Direct Debit Installment Agreements (DDIA), CADE2Marketplace (Customer Account Data Engine 2), Customer Account Data Engine 2 Operational Datastore (CADE2ODS) (Individual Taxpayer Information) and Modernized Integrated Custodial Accounting (MICA) will be onboarded on to the EDP WC2 platform. Access to data will also be provided for analytical purposes.

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

Enterprise Service Governance Board (ESGB) and Infrastructure Executive Steering Committee (IESC)

Current ELC (Enterprise Life Cycle) Milestones:

System Development/Milestone 4B

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.

EDP Workplace Community Cloud WC2 is designed a universal data hub within AWS Gov Cloud (Treasury Cloud). It will ultimately contain source data from all major tax processing systems as well as supporting data necessary to conduct the IRS mission. EDP WC2 will serve as the main source of integrated taxpayer data for analytical needs. EDP WC2 will utilize Amazon Web Services Databricks, Marketplace API, Redshift, and third-party software such as Business Objects and Informatica. EDP WC2 will also have integration with IRS common services such as NTIN. Authorized IRS personnel use analytical tools such as Business Objects and Tableau to generate reports leveraging the taxpayer data. EDP WC2 platform will host multiple datasets, for Rel 2.2 - DDIA, CADE2Marketplace, CADE2ODS (Individual Taxpayer Information) and MICA will be onboarded on to the EDP WC2 platform. Access to the DDIA, CADE2 Marketplace and MICA data will also be provided to research any anomalies that come up during the unpaid assessment statical sampling exercises. The data will only be accessible to authorized IRS personnel users that have gone through the Business Entitlement Access Request System (BEARS) approval process and only be provided access for their specific role.

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)

Delivery of governmental benefits, privileges, and services

Another compelling reason for collecting the SSN

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

The platform does not "collect" this information directly from the taxpayers. It merely receives this from authorized IRS systems, and to that extent, this data is covered by the legal statutes already in place for collection and use of this data by IRS. The SSN is the primary means of updating or querying the database by other internal systems. It is the only unique identifier associated with taxpayers, spouses, and dependents that can be used to ensure the correct records are accessed by other IRS systems. This is important when updates are made based on submitted tax forms processed by upstream systems or when information is requested from downstream systems.

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

The duration for which this data will be stored on the platform is dependent on the applicable data retention requirements and these requirements will be met. The SSN data is fundamental to the intended use by the EDP WC2 team to conduct analytical activities for financial audit purposes CADE 2 has mitigated and eliminated the SSN as an internal primary key used to link a taxpayer record thus reducing the number of times it appears in the database. CADE 2 continues to examine all system requests that state a need to access the SSN to ensure there is a specific requirement and an official IRS business need. Prior to any connections to downstream IRS systems the IRS shall examine alternative.

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
E-mail Address
Date of Birth
Standard Employee Identifier (SEID)
Protection Personal Identification Numbers (IP PIN)
Financial Account Numbers
Employment Information
Tax Account Information
Centralized Authorization File (CAF)

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.

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.

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.

SSN, First and Last name, Taxpayer signature

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

PII about individuals for Bank Secrecy Act compliance 31 USC

Information by CI for certain money laundering cases may be 18 USC

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.

Online Payment Plan obtains SBU/PII to establish a payment plan or installment agreement. OPP secures taxpayer information from databases IDRS (Integrated Data Retrieval System) and CFOL (Corporate Files Online), including social security number (SSN) and tax account information. The SBU/PII and SSN are part of the data that the Chief Financial Officer's (CFO) office needs in performing its analytical activities in order to conduct financial audit.

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

All taxpayers are authenticated by Secure Access Digital Identity (SADI) service when logging into Online Account (OLA) to validate their identity and other PII information is accurate prior to authorizing actions within OLA. When an individual sets up a payment plan, Taxpayer PII information and Payment Plan data is populated in Web Apps from authoritative IRS source systems (e.g., IDRS). Additionally, the Taxpayer is presented with their information to review and correct if it is not accurate. Any PII/SBU information provided by the Taxpayer during the plan creation is validated against IRS source systems for accuracy and completeness. Once a payment plan is created, the data is not modified as it is written to Web Apps databases/file systems prior to being securely transmitted to external systems (For example, EDP WC2 for Direct Debit Installment Agreement logs or Secure Network Drive for Letter Error Transactions). The source system(s) providing this data to the EDP is responsible for verifying the accuracy, timeliness, and completeness of this data. EDP WC2 will provide a means to ingest, store and access data securely. Rigorous testing will be conducted as data from the source is copied to the platform to ensure the copy's accuracy and completeness. Batch jobs will be run (as part of change data capture) that will determine changes between the last copy and current data from the source in order to ensure 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 00.001	Correspondence Files and Correspondence Control Files
IRS 22.062	Electronic Filing Records
IRS 37.006	Correspondence, Miscellaneous Records, and Information Management Records
IRS 24.030	Customer Account Data Engine Individual Master File
IRS 24.046	Customer Account Data Engine Business Master File
IRS 22.061	Information Return Master File
IRS 26.019	Taxpayer Delinquent Account Files
IRS 26.020	Taxpayer Delinquency Investigation Files
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: Web Applications Platform Environments
Current PCLIA: Yes
Approval Date: 1/14/2022
SA&A: No

System Name: SADI (Secure Access Digital Identity)
Current PCLIA: Yes
Approval Date: 2/15/2023
SA&A: Yes
ATO/IATO Date: 8/23/2022

System Name: Standardized IDRS Access
Current PCLIA: Yes
Approval Date: 10/26/2021
SA&A: Yes
ATO/IATO Date: 9/20/2022

System Name: CADE2 MarketPlace
Current PCLIA: Yes
Approval Date: 4/14/2022
SA&A: Yes
ATO/IATO Date: 5/21/2021

System Name: Financial Management Information system
Current PCLIA: Yes
Approval Date: 10/1/2020
SA&A: Yes
ATO/IATO Date: 9/9/2021

System Name: Redesign Revenue accounting control system
Current PCLIA: Yes
Approval Date: 3/20/2022
SA&A: Yes
ATO/IATO Date: 7/21/2021

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: 1040
Form Name: US Individual Income Tax Return

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

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: eAuthentication(eAuth)
Current PCLIA: Yes
Approval Date: 6/16/2021
SA&A: Yes
ATO/IATO Date: 10/2/2022

System Name: Web Application Platform Environment
Current PCLIA: Yes
Approval Date: 1/14/2022
SA&A: No

System Name: Standardize IDRS Access
Current PCLIA: Yes
Approval Date: 10/26/2021
SA&A: Yes
ATO/IATO Date: 9/20/2022

System Name: Tableau
Current PCLIA: No
SA&A: No

System Name: BOE
Current PCLIA: No
SA&A: No

System Name: API
Current PCLIA: No
SA&A: No

Identify the authority.

IRC Sections 6001, 6011, 6012e(a) - process taxpayer information. IRC Section 6109 - collecting SSN information cyber security compliance

For what purpose?

When online payment plans are created, the information is sent to IDRS for posting to IRS authoritative systems. DDIA authorizations are transmitted to Enterprise Data Platform (EDP WC2) for the purpose of retaining payment plans for 12 years in order to comply with legal obligations. The letter error transactions are transmitted to the shared drive environment for the purpose of Customer Service Representatives manually initiating payment plan confirmation letters to be sent to taxpayers.

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?

Yes

Is the cloud service provider (CSP) Federal Risk and Authorization Management Program (FedRAMP) certified?

Yes

Date Certified.

3/2/2020

Please identify the ownership of the CSP data.

IRS

Does the CSP allow auditing?

Yes

Who audits the CSP Data?

IRS

What is the background check level required for CSP?

Moderate

Is there a breach/incident plan on file?

Yes

Privacy laws (including access and ownership) can differ in other countries. This cloud will be Continental US (CONUS) only for:

Storage
Transmission
Maintenance

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?

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.

EDP WC2 does not collect any information directly from individuals. Data received and stored on EDP WC2 comes from approved IRS systems that have already gone through privacy verification.

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

No

Why not?

Not applicable. These aspects are covered by the source systems providing the data to EDP WC2.

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

EDP WC2 is only a repository of taxpayer information submitted directly to the IRS through other IRS applications. EDP WC2 does not interact with taxpayers directly and thus "due process" is addressed by other IRS applications that directly interact with taxpayers. To the extent that the source systems ensure "due process" regarding information access, correction, and redress, EDP WC2 as the receiver of the data from these source systems is automatically compliant.

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

IRS Contractor Employees

Contractor Users: Read Only

Contractor Managers: Read Only

Contractor System Administrators: Administrator

Contractor Developers: Read Only

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

For both letter error handling and EDP WC2 DDIA retention, access to the storage system would be maintained by the business owner. For letter error handling, the business owner would grant read only access to assigned team leads, to retrieve the list of failed letter transactions. The leads would then assign the cases to employees to work the letter failure. The listing would be cleared after the letter issued. The letter error handling process will follow established procedures as identified in IRM 5.19. 1, which requires that the letter errors be processed within 5 working days of receipt. For EDP WC2 DDIA retention, per the National Automated Clearing House Association (NACHA) requirements, all DDIA transactions are required to be maintained for 12 years. The business owner would maintain control and be solely responsible to research these logs. All contractors and employees must go through the Public Trust Clearance process before access is considered. Once cleared, an IRS employee or contractor must complete the proper request forms before access to EDP WC2 is obtained. All access must be approved, via the Business Entitlement Access Request System (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 position 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 access to an environment where a new or modified system is being tested (i.e., a non-production supporting environment) users must complete the necessary SBU data training, complete an access request form, and in some cases as outlined by the requirements set forth within the Internal Revenue Manual (IRM), submit an elevated access letter that is approved by the Associate Chief Information Officer prior to granting 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.

Online Payment Plan, Letter Error Handling and EDP WC2 DDIA Records Retention adhere to established guidelines found in Document 12990 (Rev. 11-2017) (irs.gov) RCS 28 Item 158-Online Payment Agreement (OPA). The Online Payment Agreement (OPA) is an Integrated Customer Communications Environment (ICCE) Web Applications (Web Apps) applet that allows approved taxpayers to conduct payment agreement activities on-line. (Job No. N1-058-11-11) For Online Payment Plan: Taxpayer input data would be deleted once the successful transaction has occurred. AUTHORIZED DISPOSITION Delete/Destroy any (taxpayer-entered) cached input files and data immediately following validation of receipt by the system. The data repositories and warehouses of all other source data are appropriately scheduled under other Records Control Schedules of the Internal Revenue Service. For letter error handling: Once the letter issuance has been manually processed, the record would be deleted. AUTHORIZED DISPOSITION Delete after successful entry and capture by the Individual Master File System, which is appropriately scheduled under RCS 29. Item 69(5) For EDP WC2 DDIA Records Retention: Direct Debit Installment Agreements (Form 433 Series) and related documents. These records are used by Compliance function taxpayer contact personnel to set up an agreement between the IRS and the taxpayer. The completed form permits the taxpayer to pay delinquent taxes through installment payments. AUTHORIZED DISPOSITION Destroy immediately after 12 years. All data meeting end of retention period requirements will be eliminated, overwritten, degaussed, and/or destroyed in accordance with National Archives and Records Administration (NARA)-approved disposition authorities for that system's data and done so in the most appropriate method based upon the type of storage media used in accordance with IRM 1.15.6.10. As well as General Records Schedule (GRS) 3.2, item 030 and 031 for System Access Records (AU 11).

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?

3/31/2023

Describe the system's audit trail.

The Modernized Online Payment Online (MOPP) adheres to the following process for maintaining an audit trail of the system. This policy applies to both Letter Error Handling and DDIA Authorization Log Retention: An Audit Plan has been created for this system (OLA) by the project team with the support of Enterprise Security Audit Trail (ESAT)/Security Audit and Analysis System (SAAS). The system collects legal events for Treasury Inspector General for Tax Administration (TIGTA), Criminal Investigation (CI), and the Cyber Security Data Warehouse (CSDW) to establish chain of custody for each transaction within all applications to be used as evidence and prove audit trails. It records all actions of the taxpayer/user in near-real-time and transmits to Enterprise Security Audit Trails/Security Audit & Analysis System (ESAT/SAAS) logs for Cybersecurity review. The audit trail contains the audit trail elements as required in current IRM 10.8.3, Audit Logging Security Standards. The system audit trail was a systemic account of the processes and data management on Web Apps directory and database. AUDIT will be enabled for SELECT, INSERT, UPDATE and DELETE operation on DB table to ensure all data operations are audited and Audit will be enabled on the folder on the WebApps Enterprise Services (WAES) server Redhat Enterprise Linux (RHEL) that will store the files containing failed Letter transactions and DDIA authorization logs. Current 2.2 Audit trails are under development.

PRIVACY TESTING

Does the system require a System Test Plan?

Yes

Is the test plan completed?

No

When is the test plan scheduled for completion?

3/17/2023

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?

As per the privacy requirements, testing plan is under process.

SBU DATA USE

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

No

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?

Yes

Describe the type of information derived from these efforts and the technical (e.g., audit trails) or other processes used to limit unauthorized monitoring.

By using taxpayer supplied PII and Internet Provider (IP) Addresses, the IRS will have the capability to identify, locate, and monitor taxpayers. The primary purpose of doing this is to correlate website usage with other IRS processes. For example, tracking notice response rates. With the CADE 2 database containing all individual taxpayer data the capability does potentially exist where it can be used to identity, locate, and monitor individuals and their financial information base on tax records. However, this is not the intent and audit controls are in place.

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?

Yes

Does the system have a process in place to account for such disclosures in compliance with IRC §6103(p) (3) (A) or Subsection (c) of the Privacy Act? Contact Disclosure to determine if an accounting is required.

Yes