Date of Approval: **June 22, 2022**

PIA ID Number: **7067**

SYSTEM DESCRIPTION

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

Enterprise Data Platform EDP Workplace Community, EDP WC2

Is this a new system?

Yes

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

Enterprise Services (ES)

Current ELC (Enterprise Life Cycle) Milestones:

Vision & Strategy/Milestone 0

Project Initiation/Milestone 1

Domain Architecture/Milestone 2

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.

EDP 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. Authorized IRS personnel use analytical tools like Business Objects and Tableau to generate reports leveraging the taxpayer data. This platform will host multiple projects, the first being onboarded will be Customer Account Data Engine 2 Operational Data System (CADE 2ODS).

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

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.

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.

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

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.

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?

The source system(s) providing this data to the EDP WC2 is responsible for verifying the accuracy, timeliness, and completeness of this data. CADE2ODS 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 24.030 Customer Account Data Engine Individual Master File

IRS 24.046 Customer Account Data Engine Business Master File

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

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

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: Tableau
Current PCLIA: No
SA&A: No

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 listed systems will receive SBU/PII from EDP WC2 to support their business needs including generating reports, identifying, and validating individual taxpayer information, and allowing EDP WC2 data to be available and accessible to meet additional project requirements.

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?

Yes

Identify the other source(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name: Government Printing Office
Transmission Method: Secure EFTU
ISA/MOU: No

Identify the authority.

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

Identify the Routine Use in the applicable SORN (or Privacy Act exception).

IRS 24.030 authorizes disclosure of 6103 information to a contractor, in this case 6103(n) for tax administration to carry out the Coronavirus Aid, Relief, and Economic Security (CARES) Act provisions.

For what purpose?

We are sharing information from the system with Government Printing Office vendors via secure methods for the purpose of notifying recipients of their Economic Impact Payment under the CARES Act. These vendors have a contract that includes clauses and Publication 4812 requirements for protection of PII, FTI, and SBU data, including IRC 6103(n), and their employees will be cleared, notified, and trained before receiving the data.

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.

10/31/2020

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 Contractor 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 Write

IRS Contractor Employees

Contractor Users: Read Only

Contractor Managers: Read Only

Contractor System Administrators: Administrator

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, 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.

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?

9/22/2022

Describe the system's audit trail.

The system's audit trail is currently 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?

8/15/2022

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?

Work in Progress

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.

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.

Not Applicable