

Date of Approval: **February 08, 2022**

PIA ID Number: **6618**

SYSTEM DESCRIPTION

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

Enterprise Data Platform, EDP

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

Current ELC (Enterprise Life Cycle) Milestones:

Vision & Strategy/Milestone 0

Project Initiation/Milestone 1

Domain Architecture/Milestone 2

Preliminary Design/Milestone 3

Detailed Design/Milestone 4A

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 Enterprise Data Platform (EDP) is a component-based open architecture that will deliver universal data access for users and systems at the enterprise level, meeting a range of needs. It will facilitate migration to emerging technologies, encourage open procurement competition to drive cost savings (products AND services) while maintaining control of business intelligence. This platform will host multiple projects. First project being onboarded is Modernized Individual Custodial Accounting (MICA) which will be used by Chief

Financial Officer (CFO) for reporting purposes. We will be moving data from on-premise data stores to Amazon Web Services (AWS) Govcloud (Nethub) cloud data store. This data will then be stored as a data mart in a format that is more friendly for querying and reporting. The reports will be built by CFO users using reporting tools like Business Objects and Tableau. All the AWS services being used are FedRAMP high certified. The pre-production and production environments for the platform are undergoing Authority to Operate (ATO) process following Cybersecurity production standards. Lower environments will not carry PII data. MICA data sources are: Custodial Detail Database (CDDDB), Redesigned Revenue Accounting Control System (RRACS), Financial Status Notice History (FSNH) (Integrated Data Retrieval System) The platform will also provide Artificial Intelligence (AI)/Machine Learning (ML) capabilities in the future. EDP leverages fine grained access control via AWS Identity and Access Management (IAM). The platform is embedded in a dedicated virtual private cloud (VPC) and the source data is isolated within its own subnet. Data is encrypted at rest using Key Management Service (KMS) and in transit using Transport Layer Security (TLS). While the broader vision for the platform is as described above, the current assessment is only for the first implementation (MICA) on the platform. All questions on the subsequent screens are being answered in this vein.

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).

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.

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 MICA team to conduct analytical activities for financial audit purposes.

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?

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

SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397

PII for personnel administration is 5 USC

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.

The SBU/PII and SSN are part of the data that the CFO's 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 is responsible for verifying the accuracy, timeliness, and completeness of this data. EDP 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:

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: Financial Management Information System (FMIS)

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: 4/17/2019
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?

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?

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.

9/16/2020

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?

High

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 does not collect any information directly from individuals. Data received and stored on EDP 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.

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

These are handled by the source systems which are the systems of record for the specific data. EDP receives the information from the source systems. To the extent that the source systems ensure "due process" regarding information access, correction, and redress, EDP 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 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?

Role-based access to SBU/PII will be determined and implemented by the project. Roles will be determined and granted to approved developers/users based on need.

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

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?

3/21/2022

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?

3/1/2022

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?

We have engaged with Penetration Test and Code Analysis (PTCA) to prepare for a security test plan and to schedule security testing. Cybersecurity and Security Risk management have been engaged to ensure their participation in all required activities. All customer configurable security controls will be implemented as intended and documented in the EDP System Security Plan (SSP) - currently 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: 50,000 to 100,000

Contractors: More than 10,000

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