Date of Approval: 07/29/2024
Questionnaire Number: 1322

Basic Information/Executive Summary

What is the name of your project (system, database, pilot, product, survey, social media site, etc.)?

Enterprise Data Platform - Immuta

Acronym:

EDP - I

Business Unit

Information Technology

Preparer

For Official Use Only

Subject Matter Expert

For Official Use Only

Program Manager

For Official Use Only

Designated Executive Representative

For Official Use Only

Executive Sponsor

For Official Use Only

Executive Summary: Provide a clear and concise description of your project and how it will allow the IRS to achieve its mission.

Immuta is a data access governance and policy management system. Data access policies can be defined in one central repository and pushed to one or more data stores (databases) where policies need to be enforced. Besides other capabilities, Immuta will help IRS Business Units (BU) define policies for PII data masking and NTIN (Negative Tax ID Number - which do not allow to see friends, families etc. tax related information) filtering which can be pushed to as many data stores as required. Immuta gives BUs capability to mask their PIIs. If the BUs forget to mask PII, Immuta will not mask automatically. It is the responsibility of BUs to mask their PII data. Global Policies can be set in Immuta to mask PIIs, across all databases registered, by default. Local policies can be defined to apply to specific tables. BUs will be trained to define various policies in Immuta after it goes live at the end of July 2024.

Personally Identifiable Information (PII)

Will this project use, collect, receive, display, store, maintain, or disseminate any type of Sensitive but Unclassified (SBU), Personally Identifiable Information (PII), or Federal Tax Information (FTI)?

Yes

Please explain in detail how this project uses sensitive data from inception to destruction (data lifecycle).

SEID is used to filter ITIN

Please select all types of Sensitive but Unclassified data (SBU)/Personally Identifiable Information (PII)/Federal Tax Information (FTI) that this project uses.

Standard Employee Identifier (SEID)

Cite the authority for collecting SBU/PII/FTI (including SSN if relevant).

PII for personnel administration - 5 USC

Product Information (Questions)

1.1 Is this PCLIA a result of the Inflation Reduction Act (IRA)?

No

1.3 What type of project is this (system, project, application, database, pilot/proof of concept, power platform/visualization tool)?

System

1.35 Is there a data dictionary for this system?

No

1.36 Explain in detail how PII and SBU data flow into, through and out of this system.

SEID flows into Immuta by reading it from VLDAP (Virtual Lightweight Access Protocol) periodically. Security policies like for example 1) “mask SSN” for this SEID and 2) filter a SEIDs friends & families tax records are defined in Immuta. When the user with that SEID tries to retrieve data via a report or other way, the SSN masking policy is applied, and SSNs are masked for the employee with that SEID. Similarly tax records of the friends and families of the employee with that SEID are filtered preventing him/her unauthorized access. In addition to SSN, other PII can be masked as required. Global Policies can be set in Immuta to mask PII across all databases registered by default. Local policies can be set in Immuta to mask PII to specific tables.

1.4 Is this a new system?

Yes

1.5 Is there a Privacy and Civil Liberties Impact Assessment (PCLIA) for this system?

Yes. Platform is Enterprise Data Platform.

1.6 What is the PCLIA number?

8344

1.7 What are the changes and why?

Add new application, Immuta

1.8 If the system is on the As-Built-Architecture, what is the ABA ID of the system? If this PCLIA covers multiple applications shown on the ABA, please indicate the ABA ID for each application covered separated by a comma.

This system is built under Enterprise Data Platform, ABA ID is 211416.

1.9 What OneSDLC State is the system in (Allocation, Readiness, Execution)?

Readiness

1.95 If this system has a parent system, what is the PCLIA Number of the parent system?

Enterprise Data Platform 8109

2.2 Please provide the full name of and acronym of the governance board or Executive Steering Committee (ESC) this system reports to.

Enterprise Services Governance Board (ESGB)

3.1 Does your project/system involve any use of artificial intelligence (AI), including virtual assistant, chat bot, and robotic process automation, as defined in Executive Order 13960?

No

3.3 Does this system use cloud computing?

Yes

3.31 Please identify the Cloud Service Provider (CSP), FedRAMP Package ID, and date of FedRAMP authorization.

Treasury TCloud, FR1801046750, 03/2020

3.32 Who has access to the CSP audit data (IRS or 3rd party)?

IRS

3.32 Does the CSP allow auditing?

Yes

3.33 Please indicate the background check level required for the CSP (None, Low, Moderate or High).

High

3.4 Is there a breach/incident plan on file?

Yes

3.5 Does the data physically reside in systems located in the United States and its territories and is all access and support of this system performed from within the United States and its territories?

Yes

3.6 Does this system interact with the public through a web interface?

No

3.7 Describe the business process allowing an individual to access or correct their information.

System is for internal IRS use only. IRS employees and contractors are allowed access via Business Entitlement Access Request System (BEARS) entitlement request and approval process. Approval goes through 3 stages -1) COR approval, 2) Manager approval and 3) Fulfillment team approval and fulfillment.

4.1 Who owns and operates the system (IRS Owned and Operated, IRS Owned and Contractor Operated, Contractor Owned and Operated)?

IRS Owner and Contractor Operated

4.2 If a contractor owns or operates the system, does the contractor use subcontractors?

No

4.5 Identify the roles and their access level to the PII data. For contractors, indicate whether their background investigation is complete or not.

Immuta User Admin and Audit roles can view SEID stored in Immuta.
Background investigation for all contractors is complete.

4.51 How many records in the system are attributable to IRS Employees? Enter “Under 50,000”, “50,000 to 100,000”, “More than 100,000” or “Not Applicable”.

Under 50,000

4.52 How many records in the system are attributable to contractors? Enter “Under 5,000”, “5,000 to 10,000”, “More than 10,000” or “Not Applicable”.

Under 5,000

4.53 How many records in the system are attributable to members of the public? Enter "Under 5,000", "5,000 to 10,000", "More than 10,000" or "Not applicable".

Immuta does not store such records.

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

Access to PII is determined by roles - User Admin and Audit Roles and by platform owners.

5.1 Please describe any privacy risks, civil liberties and/or security risks identified for the system that need to be resolved and what is the mitigation plan?

System audit logs are configured in AWS Cloudwatch. Cloudwatch is audit tracking service running in AWS. These logs are sent to IRS Splunk for any risks such as unauthorized access etc. Splunk is an audit log management system installed in IRS on-prem. IRS Splunk notifies appropriate IRS team for further actions. Our scope is to integrate the system audit logs to Splunk.

5.11 Is there a Risk Assessment Form and Tool (RAFT) associated with this system on file with your organization or the IRS Risk Office.

No

5.2 Does this system use or plan to use SBU data in a non-production environment?

No

Interfaces

Interface Type

Other Organization

Agency Name

AWS CloudWatch

Incoming/Outgoing

Outgoing (Sending)

Transfer Method

Amazon Web Services Platform (AWS)

Interface Type

IRS Systems, file, or database

Agency Name

Virtual Lightweight Directory Access Protocol (VLDAP)

Incoming/Outgoing

Incoming (Receiving)

Transfer Method

Other

Other Transfer Method

Lightweight Directory Access Protocol (LDAP) method is used to transfer data.

Systems of Records Notices (SORNs)

SORN Number & Name

IRS 34.037 - Audit Trail and Security Records

Describe the IRS use and relevance of this SORN.

SEID is used to retrieve business records by business units.

Please describe why a SORN is not needed.

Immuta system is not a system of record and does not store any records within itself to be retrieved by an identifier. So SORN is not applicable.

Records Retention

What is the Record Schedule System?

Non-Record

Data Locations

What type of site is this?

System

What is the name of the System?

Immuta

What is the sensitivity of the System?

Personally Identifiable Information (PII) including Linkable Data

What is the URL of the item, if applicable?

prod.immuta.edp.int.for.irs.gov

Please provide a brief description of the System.

Immuta is a data access governance and policy management system. Data access policies can be defined in one central repository and pushed to one or more data stores (databases) where policies need to be enforced. Beside other capabilities, Immuta will help to define policies for PII data masking and NTIN (Negative Tax ID Number-which do not allow to see friends, families etc. tax

related information) filtering which can be pushed to as many data stores as required.

What are the incoming connections to this System?

Incoming connection from Databricks in WC2 cloud.

What are the outgoing connections from this System?

Outgoing connection to Databricks in WC2 cloud.