Date of Approval: 04/05/2025
Questionnaire Number: 2064

Basic Information/Executive Summary

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

CMAP Voluntary Disclosure Program (VDP)

Acronym:

211625

Business Unit

Large Business and International

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.

Case Management Applications (CMAP) Voluntary Disclosure Program (VDP) system provides the Large Business & International organization the flexibility it requires to store, retrieve, update, and track taxpayer data relative to the Offshore Voluntary Disclosure Program and Other Offshore Compliance Initiatives. The main purpose of the application is to gather information from examiners concerning what they see during their offshore certification or examination. The focus is on the banks, countries, and promoters involved in offshore wealth management. This information is used to analyze offshore trends, identify countries and banks that are most involved in offshore asset movement, and to discover new offshore schemes and promotions. CMAP VDP is also used to generate statistics & reports for Large Business & International (LBI) management, the Department of Justice, and for Congressional inquiries. Due

process is provided pursuant to Title 26 United States Code (USC), Title 18 USC, and Title 31 USC.

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).

The SSN/TIN must be used to identify taxpayers and properly assess tax/penalties owed due to unreported offshore transactions, as mandated by the IRS. The SSN/TIN is also required to verify that taxpayers continue to properly report their offshore transactions. All fields (name, addresses and any taxpayer information) were vetted through a team of offshore tax experts and deemed necessary to understanding what has occurred, what is owned and where unreported offshore transactions have taken place, who promoted them, and where they might occur in the future. All data collected is required for administering the collection of unreported income from offshore taxpayer income as mandated by the IRS. The data that is collected will be information that facilitates the identification of financial information to determine the tax owed.

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

Address
Alien Registration Number
Financial Account Number
Individual Taxpayer Identification Number (ITIN)
Internet Protocol Address (IP Address)
Name
Passport Number
Social Security Number (including masked or last four digits)
Standard Employee Identifier (SEID)
Tax ID Number
Telephone Numbers

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

Information by CI for certain money laundering cases - 18 USC
PII about individuals for Bank Secrecy Act compliance - 31 USC
PII for federal tax administration - generally IRC Sections 6001 6011 or 6012
SSN for tax returns and return information - IRC section 6109

Product Information (Questions)

1 Is this PCLIA a result of the Inflation Reduction Act (IRA)?
No

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

3 What Tier designation has been applied to your system?
2

4 Is this a new system?
Yes

5 Is this system considered a child system/application to another (parent) system?
No

6 Indicate what OneSDLC State is the system in (Allocation, Readiness, Execution) or indicate if you go through Information Technology's (IT) Technical Insertion Process and what stage you have progressed to.
Readiness

7 Is this a change resulting from the OneSDLC process?
Yes

8 Please provide the full name and acronym of the governance board or Executive Steering Committee (ESC) this system reports to.
Application Development Compliance Governance Board

9 If the system is on the As-Built-Architecture (ABA), what is the ABA ID number of the system? If this PCLIA covers multiple applications shown on the ABA, please indicate the ABA ID number(s) for each application covered separated by a comma. If the system is not in the ABA, then contact the ABA (https://ea.web.irs.gov/aba/index.html) for assistance.
211603, 211625

10 If this system discloses any PII to any third party outside the IRS, 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?
Yes

11 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 and 14110?

No

12 Does this system use cloud computing?

Yes

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

Pega Platform, F1306282198 (PCFG), 3/15/2019

12.2 Does the CSP allow auditing?

Yes

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

IRS

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

Moderate

13 Does this system/application interact with the public?

No

14 Describe the business process allowing an individual to access or correct their information. (Due Process)

Information contained in the OCI (Offshore Compliance Initiative) database is received through the John Doe Summons (JDS) process. OCI database information is not accessible to taxpayers, nor is "correction" of information received applicable as the JDS respondent has provided information under a Court order.

15 Is this system owned and/or operated by a contractor?

No

16 Identify what role(s) the IRS and/or the contractor(s) performs; indicate what access level (to this system's PII data) each role is entitled to. (Include details about completion status and level of access of the contractor's background investigation was approved for.)

IRS personnel have read only access to information as needed to complete assigned examination cases. No contractors have access to the data.

17 The Privacy Act of 1974 (5 USC § 552a(e)(3)) requires each agency that maintains a system of records, to inform each individual requested to supply information about himself or herself. Please provide the Privacy Act Statement presented by your system or indicate a Privacy Act Statement is not used and individuals are not given the opportunity to consent to the collection of their PII.

The Privacy Act Statement is not applicable for the OCI (Offshore Compliance Initiative) database. Information stored in the OCI database is received through the John Doe Summons (JDS) process under a Court order.

18 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

19 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".

Not Applicable

20 How many records in the system are attributable to members of the public? Enter "Under 100,000", "100,000 to 1,000,000", "More than 1,000,000" or "Not applicable".

Under 100,000

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

All requests for access go through BEARS. Potential users must be approved by their manager and the CMAP VDP administrator. Users are not permitted access without an approved BEARS request from their authorized management official. Specific permissions (Read, Write, Modify, Delete, and/or Print) are defined on the BEARS Entitlement and set (activated) by the System Administrator prior to the user being allowed access. User privileges and user roles determine the types of data that each user has access to. Management monitors system access and removes permissions when individuals no longer require access. The CMAP VDP administrator creates and assigns "role based" user accounts to designate, control, & limit user access to PII within the application. Accounts follow the principle of "least privilege," which provides users with the least amount of access to PII data that is required to perform their business function.

23 Is there a data dictionary on file for this system? Note: Selecting "Yes" indicates an upload to the Attachment Section is required.

Yes

24 Explain any privacy and civil liberties risks related to privacy controls.

None

25 Please upload all privacy risk finding documents identified for the system (Audit trail, RAFT, POA&M, Breach Plan, etc.); click "yes" to confirm upload(s) are complete.

Yes

26 Describe this system's audit trail in detail. Provide supporting documents.

CMAP VDP application has full audit trail capabilities. Amongst other things, the system records; logins, logouts, account creation, account deletions, timeouts, & locked accounts. The audit trail assures that those who use CMAP VDP only have permission to view and use the modules their role allows. The System Administrator (SA) prepares and reviews monitoring reports based on Identity Theft and Incident Management (ITIM) established timeframes. CMAP regularly runs audits to determine accounts that no longer need access to PII or our inactive. Per IRM 10.8.1.3.1.1.2 after 120 days of inactivity, the user's account will be disabled but not removed from the system. After 365 days of inactivity, the account will be automatically deleted. Disabled or deleted accounts require that the user go through the BEARS process to regain access to the system.

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

No

Interfaces

Interface Type

Forms

Agency Name

Voluntary Disclosure Practice Preclearance Request and Application

Incoming/Outgoing

Incoming (Receiving)

Interface Type

IRS Systems, file, or database

Agency Name

Audit Information Management System (AIMS)

Incoming/Outgoing

Incoming (Receiving)

Interface Type

IRS Systems, file, or database

Agency Name

Integrated Data Retrieval System (IDRS)

Incoming/Outgoing

Incoming (Receiving)

Interface Type

IRS Systems, file, or database

Agency Name
IRS External Partner Zone (EPZ)
Incoming/Outgoing
Both
Transfer Method
Secured channel via HTTPS

Interface Type
Forms
Agency Name
Report of Foreign and Financial Bank Accounts
Incoming/Outgoing
Incoming (Receiving)

Interface Type
IRS Systems, file, or database
Agency Name
Enterprise Security Audit Trails (ESAT)
Incoming/Outgoing
Outgoing (Sending)
Transfer Method
Secured channel via HTTPS

Interface Type
IRS Systems, file, or database
Agency Name
Examination Returns Control System (ERCS)
Incoming/Outgoing
Incoming (Receiving)

Interface Type
IRS Systems, file, or database
Agency Name
Exchange of Information (EOI)-Issue Management System) (IMS)
Incoming/Outgoing
Incoming (Receiving)

Interface Type
IRS Systems, file, or database
Agency Name
Active Directory Federation Services (ADFS) On-Prem
Incoming/Outgoing
Both
Transfer Method
Secured channel via HTTPS

Interface Type

Other Organization

Agency Name

Department of Justice Swiss Bank Program

Incoming/Outgoing

Incoming (Receiving)

Agency Agreement

Yes

Agreement Name

Inter-Agency Agreement (ISA)/Memorandum of Understanding (MOU)

Transfer Method

Electronic File Transfer Utility (EFTU)

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.

OCI (Offshore Compliance Initiative) database users must request access through BEARS and receive manager approval. Users must abide by UNAX procedures with any information viewed/used during an examination.

SORN Number & Name

IRS 42.031 - Anti-Money Laundering/Bank Secrecy Act and Form 8300

Describe the IRS use and relevance of this SORN.

After research/investigation it may be determined the OCI (Offshore Compliance Initiative) database contains taxpayers subject to the BSA (Bank Secrecy Act), however the database itself does not contain BSA information.

SORN Number & Name

IRS 42.001 - Examination Administrative Files

Describe the IRS use and relevance of this SORN.

Not all information contained in the OCI (Offshore Compliance Initiative) database will result in a taxpayer audit/examination. OCI database information allows the determination of compliance/non-compliance for a taxpayer or taxpayer population. The OCI database does not contain audit/examination files or information. If information found in the OCI database is used in support of an audit/examination, Revenue Agents will follow

established documentation procedures under IRM 4.10.5.2.4 (Case File Documentation).

SORN Number & Name

IRS 42.017 - International Enforcement Program Information Files

Describe the IRS use and relevance of this SORN.

The OCI (Offshore Compliance Initiative) database may identify U.S. taxpayers with foreign business and/or foreign financial activities which fall under U.S. reporting requirements. Once a U.S. taxpayer has been identified as having a foreign business(es) and/or foreign financial activity(ies) additional research is required to determine U.S. tax compliance/non-compliance.

SORN Number & Name

IRS 42.021 - Compliance Programs and Projects Files

Describe the IRS use and relevance of this SORN.

OCI (Offshore Compliance Initiative) is tasked with identifying U.S. taxpayers involved in offshore activities. Information gathered during the John Doe Summons (JDS) process is stored in the OCI database and is used for further investigation/research in determining U.S. tax compliance/non-compliance.

Records Retention

What is the Record Schedule System?

Record Control Schedule (RCS)

What is the retention series title?

22 Tax Administration - Compliance

What is the GRS/RCS Item Number?

54

What type of Records is this for?

Both (Paper and Electronic)

Please provide a brief description of the chosen GRS or RCS item.

Offshore Compliance Initiative (OCI). This system is designed to analyze, display and report information received from summons issued to financial institutions, credit card companies, and third-party processors of financial information which may identify individuals who are illegally sheltering money offshore.

What is the disposition schedule?

AUTHORIZED DISPOSITION delete/Destroy when 20 years old, or when no longer needed for legal, audit or other operational purposes.

Data Locations

What type of site is this?

System

What is the name of the System?

Splunk

What is the sensitivity of the System?

Personally Identifiable Information (PII) including Linkable Data

Please provide a brief description of the System.

PCFG streams log data to the IRS Splunk environment via IRS EPZ, including Audit Logs, System Logs, and Monitoring Data. This ensures ongoing monitoring of platform performance and security status. Provides ongoing monitoring of platform performance and security status.

What are the incoming connections to this System?

TCP for port forwarding of logs.