

Date of Approval: 06/25/2025
Questionnaire Number: 2154

Basic Information/Executive Summary

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

Offshore Compliance Initiative

Acronym:
OCI

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.

OCI (Offshore Compliance Initiative) is a Large Business and International Division (LB&I) compliance initiative directed at bringing back into compliance with U.S. tax laws non-compliant taxpayers who maintain bank accounts, investments and/or other financial arrangements in certain Offshore Financial Centers (OFCs). These OFCs are used by taxpayers to disguise or shelter their taxable income and/or other assets. The initiative identifies U.S. persons who maintain offshore accounts, investments, and assets by reviewing the ownership and transactional records such as debit and credit cards that are linked or attached to offshore bank accounts located in any of these OFCs or correspondent bank accounts tied the offshore bank. Additionally, cryptocurrency transactional data has been secured. These ownership and transactional records are obtained from U.S. based third-party record keepers pursuant to court approved John Doe

Summonses. The OCI database is owned by the Director of Exchange and Offshore Strategies. This is not a system or application. It is a database with a front-facing GUI (graphic user interface) allowing approved users to view the data. The database is housed on the VP0TXSQLBIAD205 server. Data stored in the OCI database is manually loaded into the SQL (structured query language) database and is not transmitted to or from any other systems or applications, whether IRS owned, or other agency owned. IRS revenue agents and analysts are granted access to the OCI database by submitting a BEARS (Business Entitlement Access Request System) request for ASTARS - OCI USERS (ASTARS).

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).

OCI (Offshore Compliance Initiative) is a Large Business and International Division (LB&I) compliance initiative directed at bringing back into compliance with U.S. tax laws non-compliant taxpayers who maintain bank accounts, investments and/or other financial arrangements, including digital assets/cryptocurrency, in certain Offshore Financial Centers (OFCs). Taxpayer information, including PII, is received from the OFCs or correspondent banks is obtained from U.S. based third-party record keepers pursuant to court approved John Doe Summons (JDS). After the intake of the data from the JDS respondent(s) the data is reviewed, cleaned and loaded into the OCI database. The OCI database is a SQL (structured query language) database located on a dedicated server. Access to the OCI database is granted by submitting a BEARS (Business Entitlement Access Request System) request for ASTARS - OCI USERS (ASTARS). Approved users view the data via a front-facing GUI (graphic user interface). Data received via JDS and stored in the database is viewable to approved users. Approved users utilize the data in their assigned duties/tasks in determining taxpayer compliance as it relates to the offshore activities of the U.S. taxpayer. To date, no data has been destroyed or has been determined to no longer be needed.

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

Address

Driver's License Number

Email Address

Employer Identification Number

Financial Account Number
Global Intermediary Identification Number (GIIN)
Individual Taxpayer Identification Number (ITIN)
Internet Protocol Address (IP Address)
Name
Other
Passport Number
Preparer Taxpayer Identification Number (PTIN)
Social Security Number (including masked or last four digits)
Standard Employee Identifier (SEID)
Telephone Numbers

Please explain the other type(s) of PII that this project uses.
Date of Birth

Cite the authority for collecting SBU/PII/FTI (including SSN if relevant).
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?
3

4 Is this a new system?
No

4.1 Is there a previous Privacy and Civil Liberties Impact Assessment (PCLIA) for this project?
Yes

4.11 What is the previous PCLIA number?
8573

4.12 What is the previous PCLIA title (system name)?
Offshore Compliance Initiative

4.2 You have indicated this is not a new system; explain what has or will change and why. (Expiring PCLIA, changes to the PII or use of the PII, etc.)

This PCLIA is to update the previous expiring PCLIA 8573.

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.

Execution

7 Is this a change resulting from the OneSDLC process?

No

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

LB&I 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.

OCI 210825, ASTARS 210008

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?

No

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?

No

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)

Taxpayers do not have access to the OCI database. Data access is granted to IRS employees on a need-to-know basis. If it is determined by an IRS revenue agent or that there is potential non-compliance, an examination may be conducted, and the taxpayer will have the opportunity to provide additional information via the IDR (Information Document Request) process.

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.)

Authorized users (IRS revenue agents who have submitted and received approval via BEARS (Business Entitlement Access Request System) for ASTARS - OCI USERS (ASTARS)) have read only access to all data contained in the database. A designated DBA (database administrator) (an IRS employee in job series 2210) has write access to load the data into the database. There are no contractors with access to the database.

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.

THIS U.S. GOVERNMENT SYSTEM IS FOR AUTHORIZED USE ONLY!

Use of this system constitutes consent to monitoring, interception, recording, reading, copying, or capturing by authorized personnel of all activities. There is no right to privacy in this system. Unauthorized use of this system is prohibited and subject to criminal and civil penalties.

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".

Not Applicable

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".

100,000 to 1,000,000

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

Data access is granted on a need-to-know basis. A potential user must submit a request for access through the Online Business Entitlement Access Request System (BEARS) for management approval. Users are not permitted access without being approved by the manager on BEARS.

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 currently exist. OCI is subject to yearly FISMA (Federal Information Security Modernization Act) reporting, and should a risk be identified it is addressed during the FISMA process.

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.

User log ins are tracked and recorded in audit logs. User log ins are deactivated after 120 days of inactivity. Audit logs are attached. Any issues found during the yearly FISMA process are addressed at that time.

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

No

Interfaces

Interface Type

Other Organization

Agency Name

Financial Entities and Third-Party Record Keepers

Incoming/Outgoing

Incoming (Receiving)

Transfer Method

Electronic File Transfer Utility (EFTU)

Other Transfer Method

various by JDS respondent

Systems of Records Notices (SORNs)

SORN Number & Name

IRS 22.061 - Information Return Master File

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 PII (Personally Identifiable Information) access and UNAX (Unauthorized Access of Taxpayer Records) procedures when reviewing taxpayer data.

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.

SORN Number & Name

IRS 24.030 - Customer Account Data Engine Individual Master File

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 PII access and UNAX procedures when reviewing taxpayer data.

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 24.046 - Customer Account Data Engine Business Master File

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 PII access and UNAX procedures when reviewing taxpayer data.

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 46.002 - Criminal Investigation Management Information System and Case Files

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 Criminal Investigation procedures, however the database itself does not contain Criminal Investigation 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.

Records Retention

What is the Record Schedule System?

Record Control Schedule (RCS)

What is the retention series title?

RCS 22 Item 54-Offshore Compliance Initiative (OCI)

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.

The Offshore Compliance Initiative (OCI) Application, formerly the Offshore Credit Card Project (OCCP) 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?

RCS 22 Item 54-Offshore Compliance Initiative (OCI). (A) Inputs: Taxpayer information is received from sources external to IRS. AUTHORIZED DISPOSITION Delete/Destroy when 20 years old, or when no longer needed for legal, audit or other operational purposes. (B) System Data: Taxpayer Information in the OCI database includes account name, credit card number, all persons with signature authority over account, credit card transaction data, and other information used to determine if the taxpayer has reported all income that may be held in offshore accounts. AUTHORIZED DISPOSITION delete/Destroy when 20 years old, or when no longer needed for legal, audit or other operational purposes. (C) Outputs; Outputs included ad hoc queries of names or credit card numbers held in the system to do further research. AUTHORIZED DISPOSITION Delete/Destroy when no longer needed for legal, audit or other operational purposes, (D) System

Documentation: Owner's Manual, User Manual, Data Dictionary, Software Design Description, Software Requirements, et al.

Data Locations

What type of site is this?

System

What is the name of the System?

Offshore Compliance Initiative (OCI)

What is the sensitivity of the System?

Personally Identifiable Information (PII) including Linkable Data

What is the URL of the item, if applicable?

<https://vp0smemappociw1.ds.irsnet.gov/OCI/index.aspx>

Please provide a brief description of the System.

The OCI is a Large Business and International Division (LB&I) compliance initiative directed at bringing back into compliance with U.S. tax laws non-compliant taxpayers who maintain bank accounts, investments and/or other financial arrangements in certain Offshore Financial Centers (OFCs). These OFCs are used by taxpayers to disguise or shelter their taxable income and/or other assets. The initiative identifies U.S. persons who maintain offshore accounts, investments, and assets by reviewing the ownership and transactional records such as debit and credit cards that are linked or attached to offshore bank accounts located in any of these OFCs or correspondent bank accounts tied to the offshore bank. Additionally, cryptocurrency transactional data has been secured. These ownership and transactional records are obtained from U.S. based third-party record keepers pursuant to court approved John Doe Summonses and are reviewed by IRS researchers and analysts through use of the OCI database application.

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

What is the URL of the item, if applicable?

<https://cyberidp.enterprise.irs.gov/my.policy#>

Please provide a brief description of the System.

SPLUNK is being used to monitor OCI and is the storage area for OCI audit logs.

What are the incoming connections to this System?

None - no incoming connections from SPLUNK to OCI.

What are the outgoing connections from this System?

Audit logs from OCI are written/stored to SPLUNK.