Date of Approval: **October 27, 2022**

PIA ID Number: **7330**

SYSTEM DESCRIPTION

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

Offshore Compliance Initiative, OCI

Is this a new system?

No

Is there a PCLIA for this system?

Yes

What is the full name, acronym and milestone of the most recent PCLIA?

Offshore Compliance Initiative, OCI, O&M, # 4603

What is the approval date of the most recent PCLIA?

1/27/2020

Changes that occurred to require this update:

Expiring PCLIA

Were there other system changes not listed above?

No

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

LBI Governance Board Meeting

Current ELC (Enterprise Life Cycle) Milestones:

Operations & Maintenance (i.e. system is currently operational)

Is this a Federal Information Security Management Act (FISMA) reportable system?

Yes

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 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 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.

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:

Law enforcement and intelligence purposes

Explain why the authorized use(s) above support the new or continued use of SSNs (or tax identification numbers)

SSNs are useful in determining the identity of individuals and entities related to offshore financial accounts.

Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN's (or tax identification numbers).

There is no planned mitigation strategy to mitigate or eliminate the use of the SSN on the system.

Employer 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

Mother's Maiden Name

Certificate or License Numbers

Financial Account Numbers

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

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

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 OCI application assists the IRS in the identification of individuals and entities who have US tax liabilities. The PII is needed to identify, evaluate, and classify these entities and individuals. In our latest dataset, approximately 450 check images were determined to have SSNs/EINs on the image. This data was transcribed by the IRS, and can be included in the tabular reference data for the check image. This data would assist users of the OCI system in positively identifying the entities related to the offshore bank and crypto currency accounts.

How is the SBU/PII verified for accuracy, timeliness and completion?

OCI contains information from John Doe Summons from companies that store financial information related to offshore accounts and crypto currency transactions. Information is presented in a format as close as practicable to the format in which it was received. Prior to entering data into the OCI application, it is reviewed by data specific Subject Matter Experts and OCI developers. Adjustments and modifications are made until the SMEs and OCI developers concur that the data is accurate and appropriate for the OCI application. Data Test Plans and Test reports are approved by IRS-OCI Management prior to inclusion in the OCI application.

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 42.021 Compliance Programs and Projects Files

IRS 42.001 Examination Administrative Files

IRS 46.002 Criminal Investigation Management Information System and Case Files

IRS 24.030 Customer Account Data Engine Individual Master File

IRS 24.046 Customer Account Data Engine Business Master File

IRS 22.061 Information Return Master File

IRS 34.037 Audit Trail and Security Records

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

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?

No

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?

Yes

Identify the source that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name: Financial Entities and Third-Party Record Keepers
Transmission Method: Electronic Media
ISA/MOU 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?

No

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.

Information is collected via John Doe Summons from financial enitities that have information about offshore financial accounts.

Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information?

No

Why not?

Individuals are not identified ahead of data collection.

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

Not applicable for the OCI application. The information provided by third party sources is used to further verify tax return information collected from the individual. Procedures are in place for verifying the third-party information with the individual before making an adverse determination based on that information.

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: Administrator

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.

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.

OCI data is approved for destruction 10 years after the case is closed or when no longer needed for administrative, investigative, legal, audit, or other operational purposes, whichever is later (job No. N1-58-09-56). Retention requirements for OCI inputs, outputs, and system documentation are also stipulated under that NARA-approved Schedule (RCS) Document 12290, under RCS 18 for the Enterprise Computing Center, Item 64. Retention requirement for OCI inputs, outputs, and system documentation are also stipulated under that NARA-approved Schedule (RCS) Document 12290, under RCS 22 for Tax Administration - Compliance. Offshore Compliance Initiative (OCI). (Job No. N1-58-12-2) (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 include 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: Owners Manual, User Manual, Data Dictionary, Software Design Description, Software Requirements, et al. AUTHORIZED DISPOSITION Delete/Destroy when superseded or 5 years after the system is terminated, whichever is sooner.

SA&A OR ASCA

Has the system been through SA&A (Security Assessment and Authorization) or ASCA (Annual Security Control Assessment)?

Yes

What date was it completed?

1/25/2022

Describe the system's audit trail.

OCI Audit trail tracks each access, search, and logout of each user detailing what was searched. These records are transmitted daily to the Security Audit and Analysis System (SAAS) audit system. Transmitted reports are routinely reviewed in cyberops and the recores updloaded to SAAS are routinely reviewed accourding to their policies. ASCA reviews these procedures, process and test annually.

PRIVACY TESTING

Does the system require a System Test Plan?

Yes

Is the test plan completed?

Yes

Where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)?

OCI has undergone Unit testing, System testing, and User Acceptance testing. The system was designed, implemented, and deployed in accordance with privacy requirements and has

successfully passed testing requirements. Additionally, the system has gone through the PIA process, and has received prior PIAs (4603).

Were all the Privacy Requirements successfully tested?

Yes

Are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved?

No

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?

Developer integration testing and user acceptance testing have been completed.

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: 100,000 to 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.

The OCI system is used to assist in the identification of individuals and entities that may have unreported offshore tax liabilities. It contains financial institution information about offshore accounts. Names, addresses, DOB and other identifying information is used to help determine the potential probaility and size of the liability. The OCI team has develped application auditing in conjunction with SAAS and the procedures are tested annually through ASCA.

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