Date of Approval: 03/14/2025
Questionnaire Number: 2112

Basic Information/Executive Summary

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

Incident Management and Other DSL Treatment

Acronym:

IMODT

Business Unit

Taxpayer Services

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.

Incident Management and Other Dynamic Selected List Treatment (IMODT) Program is part of the Return Integrity & Compliance Services (RICS) under the purview of the Director of RICS, Taxpayer Services (TS). The IMODT application is a combination of both managing Incidents, along with their risk score, and managing and exporting Dynamic Selected Lists (DSL) of various Taxpayer Identifying Number (TIN) types such as Social Security Number (SSN), Employer Identification Number (EIN), Preparer's Tax Identification Number (PTIN), Electronic Filing Identification Number (EFIN). The IMODT application is used to track incidents, along with their risk score, and export all DSLs from the application to the Dependent Database (DDB). Incident sources pertain to data breaches both internally and externally to the IRS. Treatment of the various TIN types allows for selection of identity theft (IDT) returns and reduces IDT refunds.

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).

Return Integrity and Compliance Service (RICS) works as part of an overall IRS revenue protection strategy. RICS' main mission is to protect public interest by improving the IRS' ability to detect and prevent improper refunds. The Incident Management and Other DSL Treatment (IMODT) database is required to maintain PII in the database used by RICS to track incidents, along with their risk score. Preparer's Tax Identification Number (PTIN), Preparer's Employer Identification Number (PEIN), Taxpayer Identifying Numbers (TIN), Employer Identification Number (EIN), Electronic Filing Identification Number (EFIN), and Document Locator Number (DLN) are required to review income data documentation.

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

Address
Centralized Authorization File (CAF)
Email Address
Employer Identification Number
Preparer Taxpayer Identification Number (PTIN)
Social Security Number (including masked or last four digits)
Telephone Numbers

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)?

Database

3 What Tier designation has been applied to your system?

2

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?

6939

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

Incident Management and Other DSL Treatment, IMODT

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.)

Expiring PCLIA

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.

It is not in a OneSDLC State because it began prior to September 1, 2022. Per the OneSDLC guidelines, new projects as of September 1, 2022, are required to onboard to OneSDLC instead of Enterprise Life Cycle (ELC).

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.

Return Integrity and Compliance Services (RICS)

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.

211475

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?

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)

The system will allow affected parties the opportunity to clarify or dispute negative information that could be used against them. Due process is provided pursuant to 5 United States Code.

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 Employees?	Yes/No	Access Level (Read Only/Read Write/ Administrator)	
Users	Yes	Read and Write	
Managers	Yes	Read and Write	
Sys. Administrators	Yes		
Administrator Developers	Yes	Read and Write	
Contractor Employees?	Yes/No	Access Level	Background Invest. Level
Contractor Users	No		
Contractor Managers	No		
Contractor Sys. Admin.	Yes	Read and Write	Moderate
Contractor Developers	Yes	Administrator	Moderate

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 IRS notifies all individuals who file tax returns of such collection via the Privacy Act Notice which provides the legal right to ask for information under Internal Revenue Code sections 6001, 6011, and 6012(a), and their regulations. Under these sections, response is mandatory. Code section 6109 requires the individual provide an identifying number.

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".

Under 5,000

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".

More than 1,000,000

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

To obtain access to the IMODT database, all prospective users must adhere to the RICS permissions portal process. The permission portal is used for controlling access, managing (create, modify, disable, delete) user accounts, and providing administrative rights to users. All requests are handled by the RICS Service Desk and stored for auditing purposes. All application administrator and standard access requests must be authorized by the user's manager as well as a IMODT administrator. All approved database accounts will be logged. Access permissions are automatically configured to the database server after all approvals are received

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

No

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

We are not aware of any privacy risks, civil liberties and/or security risks.

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.

No

26 Describe this system's audit trail in detail. Provide supporting documents.
The database is compliant with current cyber security policies regarding audit logs as it relates to SORN 34.037 Audit Trail and Security Record System.

27 Does this system use or plan to use SBU data in a non-production environment?
No

Interfaces

Interface Type
IRS Systems, file, or database
Agency Name
Taxpayer Protection Program (TPP)
Incoming/Outgoing
Both
Transfer Method
Other
Other Transfer Method
Manual

Systems of Records Notices (SORNs)

SORN Number & Name
IRS 42.021 - Compliance Programs and Projects Files
Describe the IRS use and relevance of this SORN.
To track information relating to special programs and projects to identify noncompliance schemes

SORN Number & Name
IRS 34.037 - Audit Trail and Security Records
Describe the IRS use and relevance of this SORN.
To identify and track any unauthorized accesses to sensitive but unclassified information and potential breaches

Records Retention

What is the Record Schedule System?
Record Control Schedule (RCS)
What is the retention series title?
Income Tax Returns Filed by Individuals, Partnerships and Fiduciaries.

What is the GRS/RCS Item Number?

29 ITEM 56 - RS

What type of Records is this for?

Electronic

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

(1) Tax return records filed electronically and maintained on magnetic tape, laser optical disk, magnetic disk or other such paperless medium. (Job No. N1-58-95-1) (2) Form 8453, U.S. Individual Income Tax Declaration for an IRS e-file Return; Form 8453-OL, U.S. Individual Income Tax Declaration for an IRS e-file Online Return; Form 8453-X, Political Organization Declaration for Electronic Filing of Notice 527 Status; W-2, Wage and Tax Statements; and related schedules not conducive to electronic transmission. (Job No. N1-58-95-1) (3) Form 8633, Application to Participate in the Electronic Filing Program. (Job No. N1-58-95-1) (4) Form 9041, Application for Electronic/Magnetic Media Filing of Business and Employee Benefit Plan Returns. (Job No. N1-58-95-1) (5) Paper images of tax returns created from electronic storage medium. (Job No. N1-58-95-1) (6) Forms 8879 and 8879 (SP), IRS e-file Signature Authorization. Taxpayers use IR Form 8879 when their return is filed electronically using the practitioner Personal Identification Number (PIN) method or when the taxpayer authorizes the electronic return originator to enter the taxpayer's PIN on his/her electronically filed return. The 8879 (SP) is a Spanish language equivalent. These forms are used exclusively for individual tax filing. (Job No. N1-58-06-5)

What is the disposition schedule?

(1) Destroy on or after January 16, six years after the end of the processing year unless needed for Collection Statute Expiration Date (CSED) Extract due to a balance due. (2) Retire to Records Center beginning January 2 through March 31 following the year in which the returns were numbered and processed. Destroy on or after January 16, 6 years after the end of the processing year unless needed for Collection Statute Expiration Date (CSED) Extract due to a balance due. (3) Destroy 3 years after participant is removed from the program. (4) Destroy 3 years after participant is removed from the program. (5) Destroy after the need for the creation of the paper image has been satisfied. (6) Retire to Records Center when no longer needed for processing. Destroy on or after January 16, six years after the processing year unless needed for Collection Statute Expiration Date (CSED), TIGTA investigation, and/or Criminal Investigative Division (CID) investigation.

Data Locations

What type of site is this?

System

What is the name of the System?

IMODT

What is the sensitivity of the System?

Federal Tax Information (FTI)

Please provide a brief description of the System.

IMODT was developed by a vendor and the system audit trails have been put in place by the vendor. We have specified in the requirements for the project that an audit trail is mandatory and will contain all the audit trail elements as required by Internal Revenue Manual 10.8.3.

What are the incoming connections to this System?

Receives SBU/PII from Private Tax Practitioners (ISAC) program Encrypted.