Date of Approval: **April 17, 2019**

PIA ID Number: **3764**

SYSTEM DESCRIPTION

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

Incident Management and Other DSL Treatment, IMODT

Is this a new system?

Yes

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

Return Integrity and Compliance Services (RICS)

Current ELC (Enterprise Life Cycle) Milestones:

System Development/Milestone 4B

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

No

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.

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, Wage and Investment (W&I). IMODT application is a combination of the 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 include that pertain to data breaches both internally and externally to the IRS.

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:

Interfaces with external entities that require the SSN

When there is no reasonable alternative means for meeting business requirements

Statistical and other research purposes

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

The use or continued use of SSNs are to determine the risk based on different sources of data breaches, both external and internal, to the IRS.

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

The Office of Management and Budget Circular A-130 requires that federal agencies develop a mitigation or elimination strategy for systems that use SSNs, which the Service continues to develop strategies to meet. An exception to that requirement is when the SSN is uniquely needed to identify a user's record. The IMODT system requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer at this time. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns.

Employer Identification Number

Other Taxpayer 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

E-mail Address

Standard Employee Identifier (SEID)

Protection Personal Identification Numbers (IP PIN)

Internet Protocol Address (IP Address)

Financial Account Numbers

Tax Account Information

Centralized Authorization File (CAF)

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 (SBUList)

Protected Information - Information which if modified, destroyed or disclosed in an unauthorized manner could cause: loss of life, loss of property or funds by unlawful means, violation of personal privacy or civil rights, gaining of an unfair procurement advantage by contractors bidding on government contracts, or disclosure of proprietary information entrusted to the Government

Are there other types of SBU/PII used in the system?

Yes

Describe the other types of SBU/PII that are applicable to this system.

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), Document Locator Number (DLN), Device ID, Entity Involved, Breach Type, Referral Source

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.

Return Integrity and Compliance Service (RICS) work 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.

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

The SBU/PII information maintained in the database is provided directly from IRS files. Accuracy and completeness is inherited from the systems the data is received from.

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 34.037	Audit Trail and Security Records System

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

## For 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?

Yes

Enter the files and databases:

System Name: Taxpayer Protection Program

Current PCLIA: Yes

Approval Date: 5/23/2018

SA&A: 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?

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?

Yes

Does this system disseminate SBU/PII to other IRS Systems?

Yes

Identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name: Dependent Database

Current PCLIA: Yes

Approval Date: 9/26/2017

SA&A: No

Identify the authority

Internal Revenue Code 6109

For what purpose?

To track incidents

Does this system disseminate SBU/PII to other Federal agencies?

No

Does this system disseminate SBU/PII to State and local agencies?

No

Does this system disseminate SBU/PII to IRS or Treasury contractors?

No

Does this system disseminate SBU/PII to other Sources?

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?

Yes

How is notice provided? Was the individual notified about the authority to collect the information, whether disclosure is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects on the individual, if any, if they decide not to provide all or any of the requested information?

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 (IRC) 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.

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

No

Why not?

The legal right to ask for information is IRC sections 6001, 6011, and 6012(a), and their regulations. They say that you must file a return or statement with IRS for any tax you are liable for. Your response is mandatory under these sections. Code section 6109 requires you to provide your identifying number on the return.

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

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.

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 Write

Managers: Read Write

System Administrators: Administrator

Developers: Read Write

IRS Contractor Employees

Contractor System Administrators: Administrator

Contractor Developers: Read Write

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

In order 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.

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.

The IMODT database is unscheduled. W&I will work with the IRS Records Office to draft a request for records disposition authority for approval by the National Archives and Records Administration. When approved, disposition instructions for IMODT inputs, outputs, master files data, and system documentation will be published in Records Control Schedule (RCS) Document 12990, likely under RCS 29 for Tax Administration - Wage and Investment. W&I

proposes IMODT data disposition instructions to destroy 7 years after case is closed. The data in the IMODT database will be backed up daily and weekly for purposes of restoration GRS 3.2, Item 040 or 041 in published IRM 12829.

SA&A OR ASCA

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

No

Is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements?

Yes

Describe the system's audit trail.

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.

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)?

All test results are stored in RICS project management software. RICS .Net and Microsoft Access applications have a development (Dev) environment which is used for development and testing activities. This environment does not contain any PII data. All development and testing efforts are completed using simulated data. The development process involves developers releasing new functionality, enhancements, and defect fixes to the development environment. Each release is reviewed by the quality assurance team to ensure that both the business and technical requirements are met. All business requirement verification, functional testing, regression testing, and Section 508 testing is completed in the (Dev) environment. Issues found are remedied and subsequently released to the (Dev) environment for further testing and verification. All defects are tracked via project management software where team members can track the defects from opening to closure. The quality assurance team uses automated test scripts for regression and load testing on a secure intranet testing site for the (Dev) environment to further identify defects and verify against previous builds. Once defects are remedied, the latest code is released to the development environment. Once development is completed, User Acceptability Testing (UAT) is conducted. Upon completion of UAT, the application is released into Production Environment. The quality assurance team conducts preliminary testing in the Production environment to make sure the release meets the desired results and upon confirmation the application users are notified of the new release.

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?

The PII maintained in the IMODT database is provided directly from existing IRS systems and approved programs. Input of the data received is both systematically and manually entered into the IMODT database. Assignment of IMODT to tax examiners is manually entered by managers/administrators. Accuracy and completeness of data is inherited from the existing IRS systems.

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: Under 50,000

Contractors: Under 5,000

Members of the Public: More than 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.

Monitoring of audit logs are conducted on the system by Cyber security. Monitoring through IRS policy checkers are performed as well by Cyber security. These tools are used to ensure the system is compliant with IRS IRM regulations. If deficiencies or events are located by these tools, Cyber security can derive the circumstances of the incident and works with the system owner to mediate any events. Access to the application or system by users is managed by the 5081 process.

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