Date of Approval: **February 11, 2022**

PIA ID Number: **6647**

SYSTEM DESCRIPTION

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

Information Reporting and Document Matching, IRDM

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?

Information Reporting and Document Matching

What is the approval date of the most recent PCLIA?

2/18/2019

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.

IRDM Governance board and IRDM Executive Steering Committee (ESC).

Current ELC (Enterprise Life Cycle) Milestones:

System Development/Milestone 4B

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.

Information Return & Document Matching (IRDM) is a Small Business/Self Employed (SB/SE) Compliance application. It consists of two subsystems: IRDM Data Correlation (IRDMDC) and IRDM Business Master File Analytics (IRDMBMFA). A third subsystem IRDM Case Management (IRDMCM) was approved to be retired by the Authorizing Official on May 28, 2015. The purpose of IRDM is to assess additional corporate income tax, penalties, and interest on Form(s) 1120, 1120S, 1065, and 1041 where business returns have underreported their revenue and/or income from Form 1099s (Information Returns).

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?

Employer Identification Number

Does this system use, collect, receive, display, store, maintain or disseminate other (non-SSN) PII (i.e., names, addresses, etc.)?

No

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?

Yes

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

Form 1120, 1120S, 1065, 1041, 1099 - Misc., 1099 - K, 1099 - Int. returns and case detail & historical information.

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)

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.

IRDM compares information returns (i.e., Form 1099 series) to calendar tax year 201x Form(s) 1120, 1120S, 1065, and 1041 returns to identify discrepancies in tax return money amounts and create a universe of potential under reported cases. Preparer EIN & limited associated info is used to determine if there are fraudulent circumstances to examine further, or if there are educational opportunities to correct preparer issues.

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

The organizational records are created from information initially extracted from IRS Master File data (Business Master File (BMF) & Information Return Master File (IRMF)). This information is then imported into IRDMDC database from the Integrated Production Model (IPM) database using Informatica. The SBU/PII information exists before being stored in IRDMDC database and no NEW data is created. In other words, no IRDMDC database information transmits back to BMF, IRMF or any other system of record. All master file data corrections are done through established Internal Revenue Manual (IRM) manual procedures; there are no batch uploads from the IRDMDC database to make mass changes to any master file(s). The IRDMDC database does NOT make determinations. All determinations are completed through the Examination process with no direct correlation to the IRDMDC database.

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 24.030	Customer Account Data Engine Individual Master File
IRS 24.046	Customer Account Data Engine Business Master File

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?

Yes

Enter the files and databases:

System Name: Integrated Production Model (IPM)
Current PCLIA: Yes
Approval Date: 6/6/2019
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?

Yes

Please identify the form number and name:

Form Number: Form 1120
Form Name: US Corporation Income Tax Return

Form Number: Form 1120S
Form Name: US Income Tax Return for an S Corporation

Form Number: Form 1065
Form Name: US Return of Partnership Income

Form Number: Form 1041
Form Name: US Income Tax Return for Estates and Trusts

Form Number: Form 1099 - Misc.
Form Name: Miscellaneous Income

Form Number: Form 1099 - K
Form Name: Payment Card and Third-Party Network Transactions

Form Number: Form 1099 - Int.
Form Name: Interest Income

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: Automated Underreporter (AUR)
Current PCLIA: Yes
Approval Date: 6/12/2019
SA&A: Yes
ATO/IATO Date: 10/28/2021

Identify the authority.

Revenue Procedure 2005-32 at 4.03(1)(b) and Regulations section 1.6049-4(c)(1)(ii)

For what purpose?

The Business Under Reporter (BMF-AUR) program matches corporate tax returns (i.e., the 1120, 1120S, 1065, 1041) against third-party provided information returns (1099-MISC, 1099-K, 1099-INT, etc.) and identifies taxpayers who underreport their income.

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?

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.

In regard to the IRDM system, information is not collected directly from an individual, nor is it collected from third party sources. However, in general, the IRS notifies all individuals who file tax returns of such collection via the Privacy Act Notice in tax return instructions. When a return is selected for Examination, the taxpayer is also sent notices including the Privacy Act Notice 609 and Publication 1, Your Rights as a Taxpayer.

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

No

Why not?

In regards to the IDM system, information is not collected directly from an individual, nor is it collected from third party sources. However, in general, the IRS notifies all individuals who file tax returns of such collection via the Privacy Act Notice in tax return instructions. When a return is selected for Examination, the taxpayer is also sent notices including the Privacy Act Notice 609 and Publication 1, Your Rights as a Taxpayer.

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

The IRS implemented the Information Reporting and Document Matching (IRDM) legislation to enable additional third- party information reporting thus maximizing the IRS' capability for automated matching of data on information returns to the data submitted on business and individual tax returns. The system "IRDM" facilitates the process of selecting business cases from a pool of several million Under Reported business cases. The Business Master File BMF Underreporter (BMF AUR) organization then reviews this selection of potential returns and identified underreported (U/R) issues due to information return (IR) matching. If an Initial Contact Letter or Notice Proposing Adjustment to Income, Payments, or Credit is generated by a BMF AUR Tax Examiner, a taxpayer has the opportunity to provide additional information, such as corrected information returns or amended tax returns, to clarify, resolve or dispute the item in question prior to assessing additional tax.

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

IRS Contractor Employees

Contractor Users: Read Only

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

IRDMBMFA: Access to the data is determined by the manager based on a user's position and need-to-know. The manager will request a user be added. Permission for users to access IRDM's subsystems will be controlled via the Online Business Entitlement Access Request System (BEARS). Access permissions are based on user group assigned by the Application Administrator/Coordinator who initially sets up the IRDMBMFA user account IRDMBMFA subsystem is tied to Active Directory. IRDMBMFA users do not login into the subsystem; rather the users' credentials are passed via a handshake from Active Directory to BOE, the authenticating mechanism for the IRDMBMFA subsystem. Removal of access upon termination of employment is ensured by the user's manager through the removal of access to the IRS intranet (via Active Directory) through BEARS. IRDMDC: There is no application end user accessing the IRDMDC subsystem. System and database administrators do not have direct access to the subsystem, but rather, they access the underlying operating system.

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.

IRDM data is approved for destruction 10 years after assessment in accordance with National Archives and Records Administration (NARA) Job No. N1-58-11-17. Disposition instructions for IRDM system data, as well as system inputs, outputs and system documentation will be published in IRS Records Control Schedule (RCS) Document 12990 under RCS 32 for Electronic Tax Administration, item 45 when next updated (IRM 1.15.32 is in the processing of transitioning to Document 12990 publication format). NOTE: The business unit will coordinate with the Records and Information Management Program (RIM) Office and the Records Officer to update the disposition authority of IRDM to remove IRDMCM as a subsystem and add F-1041.

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?

10/2/2015

Describe the system's audit trail.

In the current application database, audit trailing is implemented. IRM 10.8.1 require auditing processes on each table and event. This auditing will include capturing the following: insert date and time, inserted by, update date and time, updated by. The data that IRDM receives is from internal IRS systems which are deemed reliable, and the data is validated for accuracy by the system sending the data as described in that system's PCLIA. IRDM is following the appropriate audit trail elements pursuant to current Audit Logging Security Standards.

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)?

Test results are stored in DocIT, a web-based electronic document management system powered by the enterprise standard tool Documentum. This is a tool that provides documentation control for IT projects.

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?

IRDM complies with the requirements of the current IRM 10.8.1.4.15.10 Developer Security Testing and Evaluation (07-08-2015). In addition, an Annual Security Control Assessment (ASCA) occurs annually to ensure that controls remain in place to properly safeguard

SBU/PII. The IT AD Compliance Development Branch Change Control Board (CDB CCB) has overall responsibility for managing and controlling all changes to the IRDM's subsystems. IRDM has a configuration management (CM) staffing team to handle all Configuration Management activities relating to IRDM's subsystems. A designated CM representative shall be responsible for maintaining all CM documentation, configuration identifications, configuration control, and CCB secretariat activities. The CM representative will also be responsible for monitoring all changes to IRDM's subsystems and ensuring that only the CCB approved changes are implemented in production. The CM representative will document all approved changes to the IRDM's subsystems. IRDM's subsystems utilize the IBM Rational RequisitePro management tool to maintain and track changes to the subsystems' requirements. The RequisitePro tool provides a traceability mechanism that tied the requirements to the changes implemented. Additionally, IRDM's subsystems changes are tracked and maintained in Rational ClearCase and DocIT.

SBU DATA USE

Does this system use, or plan to use SBU Data in Testing?

Yes

Was permission granted per the requirements of Form 14664, SBU Data Use Questionnaire or Form 14665, SBU Data Use Request?

Yes

Provide the date the permission was granted.

2/9/2022

Was testing performed in conformance with IRM 10.8.8 Information Technology (IT) Security, Sensitive But Unclassified (SBU) Data Policy?

Yes

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: 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?

No

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