Date of Approval: February 19, 2019 PIA ID Number: **3896**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Information Reporting and Document Matching, IRDM

2. Is this a new system? No

2.a. If no, is there a Privacy Civil Liberties Impact Assessment (PCLIA) for this system? Yes

If yes, enter the full name, acronym, and milestone of the most recent PCLIA.

Information Reporting and Document Matching, IRDM, PIA ID Number: 1540

Enter the approval date of the most recent PCLIA. 02/19/2016

If yes Indicate which of the following changes occurred to require this update (check all that apply).

No Addition of Personally Identifiable Information (PII) (PII is any information that is linked or linkable).
No Conversions
No Anonymous to Non-Anonymous
No Significant System Management Changes
No Significant Merging with Another System
No New Access by IRS employees or Members of the Public
No Addition of Commercial Data / Sources
No New Interagency Use
No Internal Flow or Collection
Yes Expiring PCLIA

Were there other system changes not listed above? No

3. 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).

3.a. Check the current Enterprise Life Cycle (ELC) Milestones (select all that apply).

No Vision & Strategy/Milestone 0
No Project Initiation/Milestone 1
No Domain Architecture/Milestone 2
No Preliminary Design/Milestone 3
No Detailed Design/Milestone 4A
Yes System Development/Milestone 4B
No System Deployment/Milestone 5
Yes Operations & Maintenance (i.e., system is currently operational)

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

A.1 General Business Purpose

5. 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).

B. PII DETAIL

6. Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any type of Sensitive but Unclassified (SBU) or Personally Identifiable Information (PII)? Yes

6.a. If 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

If yes, check all types of tax identification numbers (TIN) that apply to this system:

No	Social Security Number (SSN)
Yes	Employer Identification Number (EIN)
No	Other Taxpayer Identification Number

If SSNs apply, which of the following approved Treasury uses of the SSNs applies:

No	Security background investigations
No	Interfaces with external entities that require the SSN
No	Legal/statutory basis (e.g. where collection is expressly required by statute)
No	When there is no reasonable alternative means for meeting business requirements
No	Statistical and other research purposes
No	Delivery of governmental benefits, privileges, and services
No	Law enforcement and intelligence purposes
No	Another compelling reason for collecting the SSN

Explain why one or more of the eight authorized uses above support the new or continued use of SSNs.

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

6.b. Does this system use, collect, receive, display, store, maintain, or disseminate other (non-SSN) PII (i.e. Names, addresses, etc.)? No

6.c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? Yes

If yes, select the types of SBU

Selected	SBU Name	SBU Description
Yes	Agency Sensitive Information	Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission
No	Procurement sensitive data	Contract proposals, bids, etc.
No	Official Use Only (OUO) or Limited Official Use (LOU)	Information designated as OUO or LOU is information that: is exempt under one of the statutory Freedom of Information Act exemptions; is prohibited by other laws or regulations; would significantly impede the agency in carrying out a responsibility or function; or would constitute an unwarranted invasion of privacy.
No	Proprietary data	Business information that does not belong to the IRS
No	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
No	Physical Security Information	Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities
No	Criminal Investigation Information	Information concerning IRS criminal investigations or the agents conducting the investigations.

6.d. Are there other types of SBU/PII used in the system? Yes

If 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.

6.e. Cite the authority for collecting SBU/PII (including SSN if relevant)

Yes	PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)
No	SSN for tax returns and return information is Internal Revenue Code Section 6109
No	SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
No	PII for personnel administration is 5 USC
No	PII about individuals for Bank Secrecy Act compliance 31 USC
No	Information by CI for certain money laundering cases may be 18 USC

6.f. Has the authority been verified with the system owner? Yes

B.1 BUSINESS NEEDS AND ACCURACY

7. 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.

8. How is the SBU/PII verified for accuracy, timeliness, and completeness?

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.

C. 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.

9. 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

If yes, enter the SORN number(s) and the complete the name of the SORN(s).

SORNS Number	SORNS Name
IRS 24.030	Customer Account Data Engine Individual Master File
IRS 24.046	Customer Account Data Engine Business Master File

*IRS is required to have a published Privacy Act system of records in the Federal Register. Please identify the Privacy Act SORN(s) that cover these records. If you need additional assistance identifying the correct SORNs please email *Privacy.*

D. RESPONSIBLE PARTIES

10. Identify the individuals for the following system roles. ## Official Use Only

E. INCOMING PII INTERFACES

11. Does the system receive SBU/PII from other system or agencies? Yes

11.a. If yes, does the system receive SBU/PII from IRS files and databases? Yes

If yes, enter the files and databases.

System Name	Current PCLIA	Approval Date	SA&A?	Authorization Date
Integrated Production Model (IPM)	Yes	10/27/2017	Yes	04/01/2016

11.b. Does the system receive SBU/PII from other federal agency or agencies? No

11.c. Does the system receive SBU/PII from State or local agencies? No

11.d. Does the system receive SBU/PII from other sources? No

11.e. Does the system receive SBU/PII from Taxpayer forms? Yes

If yes, identify the forms.

Form Number	Form Name
Form 1120	US Corporation Income Tax Return
Form 1120S	US Income Tax Return for an S Corporation
form 1065	US Return of Partnership Income
Form 1041	US Income Tax Return for Estates and Trusts
Form 1099 - Misc.	Miscellaneous Income
Form 1099 - K	Payment Card and Third-Party Network Transactions
Form 1099 - Int.	Interest Income

11.f. Does the system receive SBU/PII from Employee forms (such as the I-9)? No

F. DISSEMINATION OF PII

12. Does this system disseminate SBU/PII? Yes

12.a. Does this system disseminate SBU/PII to other IRS Systems? Yes

If yes, identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name	Current PCLIA	Approval Date	SA&A?	Authorization Date
Automated Underreporter (AUR)	Yes	06/16/2016	Yes	10/28/2018

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.

12.b. Does this system disseminate SBU/PII to other Federal agencies? No

12.c. Does this system disseminate SBU/PII to State and local agencies? No

12.d. Does this system disseminate SBU/PII to IRS or Treasury contractors? No

12.e. Does this system disseminate SBU/PII to other Sources? No

G. PRIVACY SENSITIVE TECHNOLOGY

13. Does this system use social media channels? No

14. Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, Radio Frequency Identification (RFID), etc.? No

15. Does the system use cloud computing? No

16. Does this system/application interact with the public? No

H. INDIVIDUAL NOTICE AND CONSENT

17. Was (or is) notice provided to the individual prior to collection of information? No

17.b. If 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 regards 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.

18. Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information? No

18.b. If individuals do not have the opportunity to give consent, why not?
In regards 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.

19. 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.

I. INFORMATION PROTECTION

20. 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

21. The following people have access to the system with the specified rights:

IRS Employees? Yes

IRS Employees?	Yes/No	Access Level (Read Only/Read Write/ Administrator)
Users	Yes	Read-Only
Managers	Yes	Read-Only
Sys. Administrators	No	
Developers	No	

Contractor Employees? Yes

Contractor Employees?	Yes/No	Access Level	Background Invest. Level
Contractor Users	Yes	Read-Only	Moderate
Contractor Managers	No		
Contractor Sys. Admin.	No		
Contractor Developers	No		

21.a. 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 5081 (OL5081) request and approval system. 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 OL5081. 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.

I.1 RECORDS RETENTION SCHEDULE

22. Are these records covered under the General Records Schedule (GRS), or have a National Archives and Records Administration (NARA) archivist approved a Record Control Schedule (RCS) for the retention and destruction of official agency records stored in this system? Yes

22.a. If yes, how long are the records required to be held under the corresponding RCS and how are they disposed of? In your response, please include the complete IRM number 1.15.XX and specific item number and title.

IRDM data is approved for destruction 10 years after assessment in accordance wit 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 RIM Office and the Records Officer to update the disposition authority of IRDM to remove IRDMCM as a subsystem and add F-1041.

I.2 SA&A OR ASCA

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

23.a. If yes, what date was it completed? 10/02/2015

23.1 Describe in detail 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.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? Yes

24.a. If yes, was the test plan completed? Yes

24.a.1. If yes, where are 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.

24.a.2. If yes, were all the Privacy Requirements successfully tested? Yes

24.a.3. If yes, are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved? No

24.1. Describe what testing and validation activities which have been conducted or are in process 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.

K. SBU Data Use

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

25a. If yes**,** was permission granted per the requirements of Form 14664, SBU Data Use Questionnaire or Form 14665, SBU Data Use Request? Yes

If yes**,** provide the date the permission was granted. 04/28/2015

25.b. If yes, was testing performed in conformance with IRM 10.5.8, Sensitive But Unclassified (SBU) Data Policy: Protecting SBU in Non-Production Environments? Yes

L. NUMBER AND CATEGORY OF PII RECORDS

26. Identify the number of individual records in the system for each category:

26.a. IRS Employees:	Not Applicable
26.b. Contractors:	Not Applicable
26.c. Members of the Public:	More than 1,000,000
26.d. Other:	No

M. CIVIL LIBERTIES

27. Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment? No

28. Is the system information used to conduct data-mining as defined in the *Implementing the Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?* No

29. Will this system have the capability to identify, locate, and monitor individuals or groups of people? No

30. Does Computer matching occur? No

N. ACCOUNTING OF DISCLOSURES

31. 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

End of Report