Date of Approval: February 17, 2016 PIA ID Number: **1540**

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

2a. If **no**, is there a PIA for this system? Yes

If **yes**, enter the full name, acronym, PIA ID Number and milestone of the most recent PIA.

Information Reporting and Document Matching, IRDM, PIA ID Number: 426

Next, enter the **date** of the most recent PIA. 5/6/2014

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

No	Addition of PII
Yes	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

Were there other system changes not listed above? Yes

If yes, explain what changes were made. Update to remove reference to subsystem IRDMCM and add Form 1041 return and case detail

3. Check the current ELC (Enterprise Life Cycle) 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

6a. 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 who the SSN (or tax identification number) is collected on.

No	On Primary	No	On Spouse	No	On Dependent

If **yes**, check all types SSN s (or tax identification numbers) that apply to this system:

No	Social Security Number (SSN)
Yes	Employer Identification Number (EIN)
No	Individual Taxpayer Identification Number (ITIN)
No	Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
No	Practitioner Tax Identification Number (PTIN)

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

6b. Does this system contain other (non-SSN) PII that it uses, collects, receives, displays, stores, maintains, or disseminates? (i.e. Names, addresses, etc.) No

If **yes**, specify the information.

No PII Elements found.

6c. 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.

6d. 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 return and case detail & historical information

6e. 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

6f. 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? Explain how steps are taken to ensure that all information maintained by the system that is used by IRS to make any adverse determination about an individual's rights, benefits, and/or privileges is

maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination

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 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 determination are completed through the Examination process with no direct correlation to the IRDMDC database.

C. PRIVACY ACT AND SYSTEM OF RECORDS

9. Are 10 or more records containing SBU/PII maintained, stored, and/or transmitted by or through this system? Yes

9a. If **yes**, are records in the system retrieved by any personal identifier (e.g., name, SSN, Photograph, IP Address) for an individual? No

D. RESPONSIBLE PARTIES

10. Identify the individuals for the following system roles. N/A

E. INCOMING PII INTERFACES

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

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

If **yes**, enter the files and databases.

System Name	Current PIA?	PIA Approval Date	SA & A?	Authorization Date
Integrated Production Model (IPM)	Yes	12/31/2014	Yes	12/31/2014

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

11c. Does the system receive SBU/PII from State or local agency (-ies)? No

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

11e. Does the system receive SBU/PII from **Taxpayer** forms? No

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

F. PII SENT TO EXTERNAL ORGANIZATIONS

12. Does this system disseminate SBU/PII? Yes

12a. 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 PIA?	PIA Approval Date	SA & A?	Authorization Date
Business Underreporter (BMF-AUR)	No		No	

Identify the authority and 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.

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

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

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

12e. 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, cloud, global position system (GPS), biometrics, 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/is notice provided to the individual prior to collection of information? No

17b. 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

18b. If no, 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.
Contractor Users	Yes	Read-Only	Moderate
Contractor Managers	No		
Contractor Sys. Admin.	No		
Contractor Developers	No		

21a. 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.

21b. If computer matching occurs, can the business owner certify that it meets requirements of IRM 11.3.39 Disclosure of Official Information, Computer Matching & Privacy Protection Act ? Yes

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

22a. 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 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 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 ECM-R

23. Has the system been through SA&A (Security Assessment and Authorization) or ECM-R (Enterprise Continuous Monitoring Reauthorization)? Yes

23a. If **yes**, what date was it completed? 10/2/2015

23.1 Describe in detail the system s audit trail. IRDM captures: ☐Date and time that the event occurred; The unique identifier (e.g., user name, SID, application name, etc) of the user or application initiating the event; Type of event (including all identification and authentication attempts (successful and unsuccessful and commands directly initiated by the user); Subject of the event (e.g., the user, file, or other resource affected) and the action taken on that subject; and Origin of the request for identification/authentication events, Role of user, when creating the event The outcome status (success or failure) of the event. For IRDMDC, no additional information is required to be captured for this system. For IRDMBMFA, additional information to be captured for each auditable event is: Dollar Amount, Case Status Code, File Source Code, MFT Code, Name Control, Output code, Plan Number, Reason Code, Tax Period, Tax filer File Source, Tax filer TIN, Tax filer TIN Type, Campus Access, and Campus Code

J. PRIVACY TESTING

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

24b. If **yes**, Is the test plan in process or completed: Completed

24.3 If **completed/ or in process,** 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. Access to the files is controlled via Role Base Access Control. Only those authorized to access the information are allowed access. Users and developers track flaw and associated resolutions via the Knowledge Incident/Problem Service and Asset Management (KISAM) or Rational ClearQuest. IRDM developers use these tools to track identified defects, flaws that are found during testing efforts, or those discovered by users in the production environment. Rational ClearQuest also tracks developers' activities based on the code changes made to correct defects. If the flaw is determined to be a requirement change, the users and/or developers create Change Request (CR) and discuss it with the IT AD CDB CCB to gain approval. The Business Unit, on an as needed basis, determines required changes. The DBAs, system administrators, the application developers, and System Owner or system owner staff must discuss changes before they are made. The IRDM's subsystems operations staff holds regular meetings to discuss changes. All changes require management approval. The developer tests all changes to the application for proper functionality before being released Business Users initiate all other changes to the IRDM's subsystems via a Unified Work Request (UWR) and are tracked and managed via the Work Request Management System (WRMS). WRMS provides a common framework to document, control, monitor, and track requests to IT for changes to IRS information systems, and it provides the IRS with a vehicle for formal communications regarding requirements management between customer organizations and IT. Once submitted, the WRMS system maintains all of the approved changes to the application. The UWRs must include clear and complete documented requirements of the requested changes and must be coordinated with all IT personnel who may be impacted by the change. The Business Unit requestor monitors these changes to ensure that they are implemented correctly and to ensure that the requested changes do not adversely affect the system. IT AD implements configuration changes in the production environment via the transmittal process. In summary, IRDM's subsystems adhere to IRM 10.8.6 for Secure Application Development (09-30-2014). IRDM developers perform configuration management during system design, development, implementation, and operation through managing and controlling changes to the IRDM's subsystems. Only approved changes are implemented. The approved changes, security flaws and flaw resolution are documented and tracked using the IBM RequisitePro, Rational ClearCase, and/or KISAM.

24b.1. If **completed**, 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.

24b.2. If **completed**, were all the Privacy Requirements successfully tested? Yes

24.2 If **completed**, are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved? No

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. 4/28/2015

25b. **If yes**, was testing performed in conformance with IRM 10.8.8 Information Technology (IT) Security, Sensitive But Unclassified (SBU) Data Policy? Yes

L. NUMBER AND CATEGORY OF PII RECORDS

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

26a. IRS Employees: Not Applicable
26b. Contractors: Not Applicable
26c. Members of the Public: More than 1,000,000
26d. 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 9/11 Commission Recommendations 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

N. ACCOUNTING OF DISCLOSURES

30. 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