Date of Approval: July 21, 2015   PIA ID Number: **1380**

A. SYSTEM DESCRIPTION

1.   Enter the full name and acronym for the system, project, application and/or database. Information Return Systems Modernization , IRSM

2. Is this a new system? Yes

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

No	Vision & Strategy/Milestone 0
No	Project Initiation/Milestone 1
Yes	Domain Architecture/Milestone 2
No	Preliminary Design/Milestone 3
No	Detailed Design/Milestone 4A
Yes	System Development/Milestone 4B
Yes	System Deployment/Milestone 5
No	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.

IRSMDC will provide Java-based services for the new Affordable Care Act (ACA) forms in PY2016 based on ACA Release 7.0 requirements. These requirements are centered on: • Deduplication for 1094/1095 series forms to determine the authoritative submission, • Correlating corrected 1094/1095 series forms to determine the authoritative submission, • Monitoring the 1094/1095 series forms for submission completeness and indicating ready-to-use the downstream systems, • Identifying information returns that have been submitted by fraudulent or suspicious payers, • Identifying information returns that have been submitted for deceased individuals, and • Providing data access to IRDB for other processes within the enterprise. The program will implement an architecture to allow existing Information Return (IR) processing capabilities to be migrated into this new Information Returns Processing platform over the next several years. The IRSMDC project will use a service-oriented approach to allow for future use and integration of the certification functionality with the additional existing information returns (e.g., 109X series forms and W2s). IRSMDC Release 1.0 will support the following Information Return Forms: • Form 1095A – Health Insurance Market Place Statement o The IRS will receive this form from the Health Care Exchanges o Includes information about the individuals enrolled in qualified health plans • Form 1095B – Health Coverage o The tax payers will receive Form 1095B from their insurance provider or large employer o Includes information on type of coverage provided, period of coverage, and for whom coverage was provided – including dependents • Form 1094B – Transmittal of Health Coverage Information Return o A Form 1094B must be attached to any Form 1095Bs filed by an employer o This transmittal includes information on the filer's name and employer, as well as the total number of Forms 1095B submitted with this transmittal • Form 1095C – Employer-Provided Health Insurance Offer and Coverage o The employees of large employers will receive this form from their employers o There must be a single 1095C for each employee of each employer o

Reports on the type of coverage provided and identification information for each employee and their dependents • Form 1094C – Transmittal of Employer-Provided Health Insurance Offer and Coverage Information Return o A Form 1094C must be attached to any Form 1095Cs filed by an employer o Employers use 1094C to report the information about offers of health coverage and enrollment in health coverage for their employers

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 variations of SSN s (i.e. last 4 digits, etc.)?   Yes

        If **yes**, check who the SSN (or SSN variation) is collected on.

Yes	On Primary	Yes	On Spouse	Yes	On Dependent

        If **yes**, check all types SSN s (or variations of SSN s) that apply to this system:

Yes	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	Preparer Taxpayer Identification Number (PTIN)

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

        None. At this time, there is no planned mitigation strategy to eliminate the use of unmasked SSNs on the Information Return Database (IRDB). IRSM will go through the Security Assessment & Authorization (SA&A) process to ensure the system is compliant with FISMA and NIST Security Controls

    6b. Does this system contain other (non-SSN) PII that it uses, collects, receives, displays, stores, maintains, or disseminates? (i.e. Names, addresses, etc.)   Yes

        If **yes**, specify the information.

Selected	PII Element	On Primary	On Spouse	On Dependent
Yes	Name	Yes	Yes	Yes
Yes	Mailing address	No	No	No
No	Phone Numbers	No	No	No
No	E-mail Address	No	No	No
Yes	Date of Birth	Yes	Yes	Yes
No	Place of Birth	No	No	No
No	SEID	No	No	No
No	Mother's Maiden Name	No	No	No
No	Protection Personal Identification Numbers (IP PIN)	No	No	No
No	Internet Protocol Address (IP Address)	No	No	No

No	Criminal History	No	No	No
No	Medical Information	No	No	No
No	Certificate or License Numbers	No	No	No
No	Vehicle Identifiers	No	No	No
No	Passport Number	No	No	No
No	Alien (A-) Number	No	No	No
No	Financial Account Numbers	No	No	No
No	Photographic Identifiers	No	No	No
No	Biometric Identifiers	No	No	No
Yes	Employment (HR) Information	No	No	No
No	Tax Account Information	No	No	No

6c. Does this system contain SBU information that it uses, collects, receives, displays, stores, maintains, or disseminates?   <u>Yes</u>

   If **yes**, select the types of SBU

Selected	**SBU Name**	**SBU Description**
No	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)	Documents that have been marked OUO or LOU
No	Proprietary data	Business information that does not belong to the IRS
Yes	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?   <u>No</u>

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

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

6f. Has the authority been verified with the system owner?   <u>Yes</u>

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 variations) are used, explicitly explain why use of SSNs meets this criteria. Be specific.

   <u>IRSMDC will provide Java-based services for the new Affordable Care Act (ACA) forms in PY2016 (1094/1095) based on ACA Release 7.0 requirements. The need for SBU/PII is required due to business need on the system to process forms 1094/1095 and data elements.</u>

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

   <u>The system's primary function is ACA data certification through the following functionalities to ensure accuracy, relevance, timeliness, and completeness: • Deduplication for 1094/1095 series forms to determine the authoritative submission, • Correlating corrected 1094/1095 series forms to determine the authoritative submission, • Monitoring the 1094/1095 series forms for submission completeness and indicating ready-to-use the downstream systems, • Identifying information returns that have been submitted by fraudulent or suspicious payers, • Identifying information returns that have been submitted for deceased individuals, and • Providing data access to IRDB for other processes within the enterprise.</u>

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?   <u>Yes</u>

   9a. If **yes**, are records in the system retrieved by any personal identifier (e.g., name, SSN, Photograph, IP Address) for an individual?   <u>Yes</u>

   If **yes**, is there a System of Records Notice(s) or SORNs that addresses the PII records in this system?   <u>Yes</u>

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

SORNS Number	**SORNS Name**
Treas/IRS 24.030	IMF
Treas/IRS 24.046	BMF
Treas/IRS 34.037	Audit Trail and Security Records System

If **yes**, does the System of Records Notice(s) (SORN) published in the Federal Register adequately describe the records as required by the Privacy Act?   Yes

---

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**
ACA/Information Return Database (ACA/IRDB)	Yes	12/15/2014	No	

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

---

F. PII SENT TO EXTERNAL ORGANIZATIONS

12. Does this system disseminate SBU/PII?   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?   Yes

> 17a. If **yes**, how is notice provided? Was the individual notified about the authority to
> collect the information, whether such is mandatory or voluntary, the purpose for which the
> information will be used, with whom the information may be shared, and the effects, if
> any, if they decide not to provide any of the requested information?
> The system will allow affective parties the opportunity to clarify or dispute negative information that
> could be used against them. Due process is provided pursuant to 5 USC.

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?   The system uses data entered from tax returns filed by taxpayers. They are
> notified of such collection by the Privacy Act Notice in the tax return instructions.

19. How does the system or business process ensure due process regarding information access,
correction and redress?
The system uses data entered from tax returns filed by taxpayers. They are notified of such
collection by the Privacy Act Notice in the tax return instructions.

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	No	
Managers	No	
Sys. Administrators	Yes	Administrator
Developers	Yes	Read And Write

Contractor Employees?   Yes

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

> 21a. How is access to SBU/PII determined and by whom? There will be no direct access to SBU/PII
> data through the IRSM system because IRSM does not provide access to end users.

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 ? <u>Yes</u>

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?   <u>No</u>

    22b. If **no**, how long are you proposing to retain the records? Please note, if you answered no, you must contact the IRS Records and Information Management Program to initiate records retention scheduling before you dispose of any records in this system.

    <u>IDC is non-recordkeeping and no other records scheduling actions are required. IDC performs data certification services that validate and check IRDB data quality for providing to recordkeeping systems downstream, as appropriate.</u>

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)?   <u>No</u>

    23c. If **no**, is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements?   <u>Yes</u>

23.1 Describe in detail the system s audit trail.   <u>IRSMDC is non-recordkeeping and no other records scheduling actions are required. IRSMDC performs data certification services that validate and check IRDB data quality for providing to recordkeeping systems downstream, as appropriate. The system's audit trail capability has not been formulated at this time.</u>

J. PRIVACY TESTING

24. Does the system require a <u>System Test Plan</u>? <u>Yes</u>

    24b. If **yes**, Is the test plan in process or completed: <u>In Process</u>

    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?
    <u>Security testing to be scheduled but not yet started</u>

K. SBU Data Use

25. Does this system use, or plan to use SBU Data in Testing?   <u>No</u>

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