

NOTE: The following reflects the information entered in the PIAMS website.

---

## A. SYSTEM DESCRIPTION

---

Authority: Office of Management Budget (OMB) Memorandum (M) 03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 & PVR #10- Privacy Accountability and #21-Privacy Risk Management

---

Date of Approval: January 14, 2015

PIA ID Number: **1039**

---

1. What type of system is this? Legacy

1a. Is this a Federal Information Security Management Act (FISMA) reportable system? No

---

2. Full System Name, Acronym, and Release/Milestone (if appropriate):

Microfilm Replacement System , MRS

---

2a. Has the name of the system changed? No

If yes, please state the previous system name, acronym, and release/milestone (if appropriate):

---

3. Identify how many individuals the system contains information on

Number of Employees: Under 50,000

Number of Contractors: Not Applicable

Members of the Public: Not Applicable

---

4. Responsible Parties:

---

NA

---

5. General Business Purpose of System

---

The MRS application is a compilation of routines/programs that extract data, including privacy information (such as Taxpayer Identification Number (TIN), Social Security Number (SSN), Address, etc.) from the Individual Master File (IMF) and Business Master File (BMF) housed on an IBM Mainframe at the Enterprise Computing Center – Martinsburg (ECC-MTB), which is part of the MITS-21 GSS. Each program submits a transcript request from either the Service Center or area office requesting specific information from the IMF or BMF. The program then runs overnight and extracts data from the pertinent Master File, reformats it into Taxpayer Information File (TIF) and Research Data File (RDF) format, and returns it to the Service Centers for editing and distribution to the requester. The MRS application also provides extracted Master File information for Disclosure. There is no direct user interface, as all information input into the system is handled through the Job Control Language (JCL) routines associated with the coding. The daily JCL is handled through an automated system (Control-M). ECC-MTB administrators have access to the automated system and the daily JCL. Most information requested is returned the following day. The only exception to this rule is the information obtained from the mainframe located at ECC-MTB (Modernization & Information Technology Services (MITS)-21 GSS). This information is specific to an individual, including SSN, address, data of birth, etc. and is obtained from the Social Security Administration (SSA). All information requested from and obtained from SSA is sent to the MITS-21 mainframe via CONNECT:Direct. This information is then extracted from the mainframe to MRS during its scheduled routine. As there is no direct connection between SSA and MRS, no Memorandum of Understanding (MOU) is required.

6. Has a PIA for this system, application, or database been submitted previously to the Office of Privacy Compliance? (If you do not know, please contact \*Privacy and request a search) Yes

6a. If **Yes**, please indicate the date the latest PIA was approved: 11/28/2011 12:00:00 AM

---

6b. If **Yes**, please indicate which of the following changes occurred to require this update.

- System Change (1 or more of the 9 examples listed in OMB 03-22 applies) (refer to PIA Training Reference Guide for the list of system changes) No
- System is undergoing Security Assessment and Authorization No

6c. State any changes that have occurred to the system since the last PIA

Non FISMA Reportable Due to the nature of a level 3, there is no security risk or impact to the organization and therefore does not require documentation within a FISMA boundary.

7. If this system has an Exhibit 53 or Exhibit 300 please provide the Unique Project Identifier (UPI) number (XXX-XX-XX-XX-XXXX-XX). Otherwise, enter the word 'none' or 'NA'. NA

**B. DATA CATEGORIZATION**

Authority: OMB M 03-22 & PVR #23- PII Management

8. Does this system collect, display, store, maintain or disseminate Personally Identifiable Information (PII)? Yes

9. Indicate the category that best describes the source that provides or originates the PII collected, displayed, stored, maintained or disseminated by this system. Most common categories follow:

Taxpayers/Public/Tax Systems Yes

Employees/Personnel/HR Systems No

Other Source:

Other No

10. Indicate all of the types of PII collected, displayed, stored, maintained or disseminated by this system. Then state if the PII collected is on the Public and/or Employees. Most common fields follow:

TYPE OF PII	Collected?	On Public?	On IRS Employees or Contractors?
Name	Yes	Yes	No
Social Security Number (SSN)	Yes	Yes	No
Tax Payer ID Number (TIN)	Yes	Yes	No
Address	Yes	Yes	No
Date of Birth	Yes	Yes	No

Additional Types of PII: Yes

<u>PII Name</u>	<u>On Public?</u>	<u>On Employee?</u>
• Taxpayer Name	No	No
• Address	No	No
• Date of Birth Certificate Number	No	No
• Prior Date of Birth	No	No
• Sex	No	No
• Citizenship Type	No	No
• Mothers And Fathers Name	No	No
• Disability Freeze Indicator	No	No

10a. What is the business purpose for collecting and using the SSN ?

SSA provides NUMIDENT (Number Identification) data to the Master File, which is located on the MITS-21 GSS. Master File interconnects with MRS to provide the following NUMIDENT data from SSA: • Taxpayer Name • Address • Date of Birth • Place of Birth • Birth Certificate Number • Prior Date of Birth • Date of Birth • Change Indicator • Sex • Race • Citizenship Type • Mother’s Name • Father’s Name • Disability Freeze Indicator

If you answered **Yes** to Social Security Number (SSN) in question 10, answer **10b**, **10c**, and **10d**.

---

10b. Cite the authority that allows this system to contain SSN's? (e.g. specific regulations, statutes, etc.)

IRC 6109(a) IRM 10.2.1.4 IRC 6103, 7213, 7217 and 7431

---

10c. What alternative solution to the use of the SSN has/or will be applied to this system? (e.g. masking, truncation, alternative identifier)

No alternate solution to the use of the SSN in reviewing document data is productive.

---

10d. Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of Social Security Numbers on this system?

There is no planned mitigation strategy at this time.

---

Describe the PII available in the system referred to in question 10 above.

SSA provides NUMIDENT (Number Identification) data to the Master File, which is located on the MITS-21 GSS. Master File interconnects with MRS to provide the following NUMIDENT data from SSA:

• Taxpayer Name • Address • Date of Birth • Place of Birth • Birth Certificate Number • Prior Date of Birth • Date of Birth • Change Indicator • Sex • Race • Citizenship Type • Mother's Name • Father's Name • Disability Freeze Indicator

11. Describe in detail the system's audit trail. State what data elements and fields are collected. Include employee log-in information. If the system does not have audit capabilities, explain why an audit trail is not needed.

Audit trail archival logs for data are retained in accordance with IRM 1.15, unless otherwise specified by a formal Records Retention Schedule developed in accordance with IRM 1.15, Records Management. Any changes from the retention requirements stated in LEM 10.8.3 are part of the audit plan and approved by Business System Owner and Cybersecurity. The IRS retains audit log data, along with other system-specific records, as specified by a system records retention schedule for the system in question. See IRM 1.15, Records Management, for specific guidance regarding system records retention schedules. Audit logs may be retained up to seven (7) years, per IRM 1.15. IRM 1.15 has precedence over this IRM for systems covered by IRM 1.15. Table 5-5 delineates the audit log retention requirements deployed by systems based on the FIPS 199 overall security categorization for the system. IRS systems (including applications, databases, network devices, and operating systems) which are not covered under the scope of a system records retention schedule adheres to the following default log retention policy:  Online computer audit logs are retained for a minimum of two (2) days prior to archival.  Archival logs are retained for a minimum of 6 months.  An Information System Owner may establish a system-level business requirement to retain online or archival logs for a longer period than the minimums specified above. The amount of time that the system-level business wants to retain logs should be placed in the Audit Plan.  IRS organizations or individuals (such as System Administrators) that desire shorter minimum log retention periods than those specified above must submit a Deviation request to justify the shorter retention period. Database audit data is not required to be local to the database for the period of retention, but is available for historical analysis if needed. Audit data is only be readable by personnel authorized by the SecSpec. At the end of the retention period, the audit logs are reviewed to determine if the logs require archival at the Federal Records Center or destruction. Additional guidance is provided in IRM 1.15. The application relies on the MITS-21 GSS and MITS-22 GSS, which it resides on, for the implementation of this control. Refer to the MITS-21 GSS and MITS-22 GSS SSPs for additional information. Specifically, the MRS application is a compilation of batch programs with no direct user interface. There are no users of the application, only developers (BMF and IMF) and system administrators, both of whom cannot access MRS data. Developers and system administrator accounts are handled via RACF and fall under the responsibility of MITS EOps administrators. Since there are no users of the application, and data is just being passed from one point to another without any user interaction, there is no requirement to maintain audit logs at the application level.

11a. Does the audit trail contain the audit trail elements as required in current IRM 10.8.3 *Audit Logging Security Standards*? Yes

12. What are the sources of the PII in the system? Please indicate specific sources:

a. IRS files and databases: Yes

If **Yes**, the system(s) are listed below:

<u>System Name</u>	<u>Current PIA?</u>	<u>PIA Approval Date</u>	<u>SA &amp; A?</u>	<u>Authorization Date</u>
Notice Review Processing System (NRPS)	Yes	01/02/2014	Yes	03/06/2014
Individual Master File (IMF)	Yes	05/02/2014	Yes	11/15/2012
Business Master File (BMF):	Yes	05/28/2014	Yes	05/23/2013
Transcript Research System (TRS):	No	05/28/2014	No	05/23/2013
Dependent Database (DEPDB)	Yes	12/04/2014	Yes	03/02/2012

b. Other federal agency or agencies: No

c. State and local agency or agencies: No

d. Third party sources: No

e. Taxpayers (such as the 1040): No

f. Employees (such as the I-9): No

g. Other: No If **Yes**, specify:

---

### C. PURPOSE OF COLLECTION

---

*Authorities: OMB M 03-22 & Internal Revenue Manual (IRM) 10.8.8, IT Security, Live Data Protection Policy & PVR #16, Acceptable Use*

13. What is the business need for the collection of PII in this system? Be specific.

Each data item is required for the business purpose of the system. Each data item being extracted from IMF and BMF is needed for inclusion in the various batch processes that are sent out to TRS, and DEPDB. The MRS batch processes reformat the extracted IMF and BMF data into TIF and RDF format and then and returns it to the Service Centers for editing and distribution to the requester.

---

### D. PII USAGE

---

*Authority: OMB M 03-22 & PVR #16, Acceptable Use*

14. What is the specific use(s) of the PII?

To conduct tax administration No

To provide taxpayer services No

To collect demographic data No

For employee purposes No

Other: No

*If other, what is the use?*

---

**E. INFORMATION DISSEMINATION**

---

Authority: OMB M 03-22 & PVR #14- Privacy Notice and #19- Authorizations

15. Will the information be shared outside the IRS? (for purposes such as computer matching, statistical purposes, etc.) No
16. Does this system host a website for purposes of interacting with the public? No
17. Does the website use any means to track visitors' activity on the Internet?  
If yes, please indicate means:

	YES/NO	AUTHORITY
Persistent Cookies	_____	_____
Web Beacons	_____	_____
Session Cookies	_____	_____
Other:	_____	<i>If other, specify:</i> _____

---

**F. INDIVIDUAL CONSENT**

---

Authority: OMB M 03-22 & PVR #15- Consent and #18- Individual Rights

18. Do individuals have the opportunity to decline to provide information or to consent to particular uses of the information? Not Applicable
- 18a. If **Yes**, how is their permission granted?

19. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action? Yes

- 19a. If **Yes**, how does the system ensure "due process"?

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.

20. Did any of the PII provided to this system originate from any IRS issued forms? No

- 20b. If **No**, how was consent granted?

Written consent	_____
Website Opt In or Out option	<u>No</u>
Published System of Records Notice in the Federal Register	<u>No</u>
Other:	<u>No</u>

---

**G. INFORMATION PROTECTIONS**

---

Authority: OMB M 03-22 & PVR #9- Privacy as Part of the Development Life Cycle, #11- Privacy Assurance, #12- Privacy Education and Training, #17- PII Data Quality, #20- Safeguards and #22- Security Measures

21. Identify the owner and operator of the system: IRS Owned and Operated

- 21a. If Contractor operated, has the business unit provided appropriate notification to execute the annual security review of the contractors, when required?

22. The following people have use of the system with the level of access specified:

	Yes/No	Access Level
IRS Employees:	<u>No</u>	
Users		<u>No Access</u>
Managers		<u>Read Only</u>

System Administrators	Read Only
Developers	Read Write
Contractors:	No
Contractor Users	
Contractor System Administrators	
Contractor Developers	
Other:	No

If you answered yes to contractors, please answer **22a**. (All contractor/contractor employees must hold at minimum, a "Moderate Risk" Background Investigation if they have access to IRS owned SBU/PII data.)

22a. If the contractors or contractor employees act as System Administrators or have "Root Access", does that person hold a properly adjudicated "High Level" background investigation?

23. How is access to the PII determined and by whom?

Users: MRS does not have any end-users. Managers: MRS does not have any managers. System Administrators: MRS does not have any System Administrators. MRS does not maintain databases. Developers: Have read-only access to the production data via the privileges assigned to their Resource Access Control Facility (RACF) profile. Others: None. There are no outside contractors working on the MRS applications. MRS does not have any end-users. The Application Developer must complete a Master File Form 104 to request read access to production data which also has to be approved by the manager. The application developers are users of the development IBM Masterfile platform located in ECC MTB. An Online 5081 (OL 5081) request is required for access to the IBM Masterfile platform. Yes. Individual Master File (IMF): IMF files are read (read only) by MRS via batch processing on a daily basis. Data is on the same system as MRS. Data access is through standard IBM data access routines. IMF provides the following PII to MRS: TIN, SSN, taxpayer name, taxpayer address, and tax year. Four batch programs are associated with IMF and MRS. Business Master File (BMF): BMF files are read (read only) by MRS via batch processing on a daily basis. Data is on the same systems as MRS. Data access is through standard IBM data access routines. BMF provides the following PII to MRS: TIN, SSN, taxpayer name, taxpayer address, and tax year. Nineteen batch programs are associated with BMF and MRS. Transcript Research System (TRS): TRS is a subsystem of IDRS. TRS sends Master File Transcripts (MFTRA) requests to and receives replies from MRS via CONNECT:Direct. MFTRA requests come to the IBM Masterfile system through IDRS. The data is stored in a dataset that is accessed by MRS. The data to be returned to TRS is written to a dataset that is accessed by CONNECT:Direct. The data received is used for verification purposes and includes the following: TIN/SSN, taxpayer name, and taxpayer address. Dependent Database (DEPDB): DEPDB sends requests to, and receives replies from MRS via batch processing. Data is on the same systems as MRS. Data access is through standard IBM data access routines. The data shared between DEPDB and MRS is used for verification purposes and includes the following: TIN/SSN, taxpayer name, and taxpayer address. Disclosure (non-application): Disclosure sends requests to, and receives replies from MRS via batch processing. Data is on the same systems as MRS. Data access is through standard IBM data access routines. The data shared between Disclosure and MRS is used for verification purposes and includes the following: TIN/SSN, taxpayer name, and taxpayer address. CTRL-D is used to print output reports from this system. ECC-MTB Transcripts (non-application): ECC-MTB sends requests to, and receives replies from MRS via batch processing. Data is on the same systems as MRS. Data access is through standard IBM data access routines. The data shared between Disclosure and MRS is used for verification purposes and includes the following: TIN/SSN, taxpayer name, and taxpayer address. Individual Master File (IMF) Business Master File (BMF) Transcript Research System (TRS) Part of the Integrated Data Retrieval System (IDRS) Dependent Database (DEPDB) The Social Security Administration (SSA) NUMIDENT database sends weekly updated files to the IRS Master File System via a virtual private network (VPN) tunnel connection. MRS obtains the data from the Master File System via Connect Direct. Although this data is coming from an external source (SSA), the data first comes to Master File which is a different system residing on the same mainframe as MRS. The data is picked up from Master File and is sent to the mainframe where the MRS application is located.

24. How will each data element of SBU/PII be verified for accuracy, timeliness, and completeness?

Accuracy, completeness, and validity checks are incorporated into the application to account for the most probable errors and for errors that could potentially propagate into good data. Checks include, but are not limited to, numerous fields on the input data, record type to file type associations, input file names associated with JCL control card. Data validity checking is done at the master file level with no data altering by the MRS application.

---

25. 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

---

25a. 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.

MRS system data is approved for deletion/destruction when obsolete or no longer needed. MRS relies on the IBM mainframe and the MITS-21 and MITS-22 General Support Systems (GSSs) for eliminating the data, as appropriate. The National Archives and Records Administration (NARA) approved these disposition instructions under Job No. N1-58-09-49 (approved 11/23/09). These instructions are published in Records Control Schedule (RCS) Document 12990 under RCS 19 for Enterprise Computing Center - Martinsburg (ECC-MTB), Item 60.

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.

---

26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.

The application does not interconnect to any system or application external to the IRS. Memorandum of Understandings (MOU)/Interconnection Security Agreements (ISA) are not required for internal interconnections; therefore, there are no existing MOUs/ISAs associated with this application.

26a. Next, explain how the data is protected in the system at rest, in flight, or in transition.

It was determined that MRS does not transmit data, therefore security controls was not applicable for this system. As a result, the implementation status of control security controls has changed from Risk Based Decision to Not Applicable. Currently, IRS security policy does not require applications that are internally facing to the IRS network to implement security controls. These applications should not have any external interconnections with other applications outside of the IRS firewalls. Therefore, these controls are implemented as Risk Based Decisions for internally facing applications.

---

27. Has a risk assessment (e.g., SA&A) been conducted on the system to ensure that appropriate security controls have been identified and implemented to protect against known risks to the confidentiality, integrity and availability of the PII? No

---

28. Describe the monitoring/evaluating activities undertaken on a regular basis to ensure that controls continue to work properly in safeguarding the PII.

Non FISMA Reportable

---

29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 - *IT Security, Live Data Protection Policy*? Not Applicable

---

29a. Has approval been received from the Office of Privacy Compliance to use Live Data in testing (*if appropriate*)?

29b. If you have received permission from the Office of Privacy Compliance to use Live Data, when was the approval granted?

---

## **H. PRIVACY ACT & SYSTEM OF RECORDS**

Under the statute, any employee who knowingly and willfully maintains a system of records without meeting the Privacy Act notice requirements is guilty of a misdemeanor and may be fined up to \$5000.

*Authority: OMB M 03-22 & Privacy Act, 5 U.S.C. 552a (e) (4) & PVR #13-Transparency*

---

30. Are 10 or more records containing PII maintained/stored/transmitted through this system? Yes

---

31. Are records on the system retrieved by any identifier for an individual? (Examples of identifiers include but are not limited to Name, SSN, Photograph, IP Address) Yes

31a. If **YES**, the System of Records Notice(s) (SORN) published in the Federal Register adequately describes the records as required by the Privacy Act? Enter the SORN number and the complete name of the SORN.

No SORN Records found.

## I. ANALYSIS

Authority: OMB M 03-22 & PVR #21- Privacy Risk Management

---

32. What choices were made or actions taken regarding this IT system or collection of information as a result of preparing the PIA?

Resulted in the removal of PII from the system (e.g., SSN use reduced/eliminated)

No

Provided viable alternatives to the use of PII within the system

No

New privacy measures have been considered/implemented

No

Other:

No

32a. If **Yes** to any of the above, please describe:

NA