Automated Non Master File System (ANMF) – Privacy Impact Assessment

PIA Approval Date – June 26, 2009

System Overview

Automated Non–Master File (ANMF) system (formerly MARS, Manual Accounting Replacement System) tracks receivables from taxpayers for Non-Master File (NMF) assessments and generates billing notices to the taxpayers. The application guides each account to one of the several paths in which a determination is made as to whether collection procedures will take place or the account will be closed. The NMF Unit has sole access for posting of taxpayer information to the system, but the application is also accessible to the Revenue Accounting Control System (RACS) Unit for block control input and journal update. Other Internal Revenue Service (IRS) functions are restricted to research capability. ANMF supports accounting for assessment, liabilities, payments, and credits for transactions not compatible with master file processing, timeliness or data.

Systems of Records Notice (SORN):

- IRS 22.060 – Automated Non-Master File (ANMF)
- IRS 34.037 – Audit Trail and Security Records System

Data in the System

1. Describe the information (data elements and fields) available in the system in the following categories:

A. Taxpayer – Taxpayer's name, address, Social Security Number (SSN) or Employee Identification Number, tax liability, payment information and balance due amount is input from tax returns, payment and adjustment documents that cannot be processed to the Individual, Business, or Employee Plans Master Files.

B. Employee – An OL5081 is required of IRS users requesting access to the ANMF application and must be signed by an immediate manager. Each user is assigned a unique User ID and password to access ANMF. No SEID (Standard Employee Identifier) is used for accessing ANMF.

C. Audit Trail Information – The audit trail information is the User ID (not SEID) which is used in accordance with the IRS Information Technology (IT) Security, Policy and Guidance Internal Revenue Manager (IRM) 10.8.1

D. Other – DHHS (Department of Health & Human Services) provides to the IRS, the obligor's SSN and address, amount of arrearage, and case control number via paper document.

2. Describe/identify which data elements are obtained from files, databases, individuals, or any other sources.

A. Taxpayer – Taxpayer SSN, taxpayer correspondence, taxpayer entity information. Tax account data will be available on a need to know basis. The employee would research the tax modules for pertinent information to resolve issue.

B. Employee – An OL5081 is required of IRS users requesting access to the ANMF application and must be signed by an immediate manager. Each user is assigned a unique User ID and password to access ANMF. No SEID (Standard Employee Identifier) is used for accessing ANMF. No other employee information is captured other than what is described above in 1C; The audit trail information is the employee login which is used in accordance with the IRS Information Technology (IT) Security, Policy and Guidance IRM 10.8.1.

C. Other Federal Agencies – DHHS (Department of Health & Human Services) provides to the IRS, the obligor's SSN and address, amount of arrearage, and case control number via paper document

3. Is each data item required for the business purpose of the system? Explain.
Yes. Each data item is necessary to conduct tax assessments and collections.

4. How will each data item be verified for accuracy, timeliness, and completeness?
Data is original input and key verified by two separate operators. System checks exist for validation of data and subject reviews/internal controls.

5. Is there another source for the data? Explain how that source is or is not used.
No. There is no other source for the data.

6. Generally, how will data be retrieved by the user?
Authorized users are able to query based on the taxpayer name, SSN or EIN.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?
Yes. Data is retrievable by the taxpayer's name, SSN, or EIN on a "need-to-know" basis.

Access to the Data

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?
Only IRS personnel can have access to ANMF which are Users, Managers, Database Administrator's, System Administrators, Developers, and HQ Analysts.

Role: Data Manager
Permission: Read, Write, Query, Delete

Role: NMF User
Permission: Read, Write, Query, Delete

Role: Journal User
Permission: Read, Query,

Role: Data Administrators (DBA)
Permission: Read, Write, Query, Delete

Role: Accounting User
Permission: Read, Query

Role: Research User
Permission: Read, Query

Role: Index Card User
Permission: Read, Query

9. How is access to the data by a user determined and by whom?
A unique ANMF user-ID and password is required for system authentication. An OL5081 is required of IRS users requesting access to the ANMF application and must be signed by an immediate manager. The OL5081 process ensures that the user identifier is issued to the intended party and that user identifiers are properly archived. Once the request is signed by the immediate manager, the request is submitted to the HQ ANMF Analyst for pre-approval. The pre-approval process includes a validity check and the assignment of an application role/level of access, minimally required for the user to accomplish their assigned tasks. The request is then submitted to the system administrator, who adds the user to ANMF and the predetermined application role.

10. Do other IRS systems provide, receive, or share data in the system? If YES, list the system(s) and describe which data is shared.
Yes. ANMF only provides data to the other IRS systems listed below:

- Automated Lien System (ALS) – ANMF only provides lien information for Field Revenue Officers to track lien assignments and due dates such as taxpayer name, address, and telephone number.
- Desktop Integration (DI) – replaces the Integrated Case Processing system and permits research access only to the ANMF database.
- Enforcement Revenue Information System (ERIS) – ANMF only provides data for the development of enforcement revenue analysis for taxation management such as taxpayer name, address, and telephone number.
- Financial Management Information System (FMIS) – ANMF only provides data for the support and preparation of the revenue and refund reports such as taxpayer name, address, and telephone number.
- Interim Revenue Accounting Control System (IRACS) – ANMF only provides data for automatic journalization of ANMF transactions to the respective general ledger accounts and Form 23C, Certificate of Assessments such as taxpayer name, address, and telephone number.
- Service Center Control File (SCCF) – ANMF only provides data to systemically post the Good Block Proof Record to the Non-Master File (NMF) SCCF such as taxpayer name, address, and telephone number.

11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?
Yes.

Service Center Control File (SCCF)
- Privacy Impact Assessment (PIA) – March 18, 2009
- Authority To Operate (ATO) – June 7, 2009 (expected)

Automated Lien System (ALS)
- Privacy Impact Assessment (PIA) – April 10, 2007

- Authority To Operate (ATO) – March 24, 2008

Enforcement revenue Information (ERIS)
- Privacy Impact Assessment (PIA) – January 26, 2007
- Authority To Operate (ATO) – June 30, 2008

Interim Revenue Accounting Control System (IRACS)
- Privacy Impact Assessment (PIA) – April 11, 2006
- Authority to Operate (ATO) – February 28, 2008

Financial Management Information System (FMIS)
- Privacy Impact Assessment (PIA) – January 30, 2009
- Authority to Operate (ATO) – May 8, 2009

Desktop Integration (DI) – N/A

12. Will other agencies provide, receive, or share data in any form with this system?
No. No other agencies provide, receive, or share data in any form with this system. DHHS (Department of Health & Human Services) provides to the IRS, the obligor's SSN and address, amount of arrearage, and case control number via paper document.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?
All procedures for eliminating the data at the end of the retention period are compliant with the Internal Revenue Service's Record Control Schedule for Tax Administration – Wage and Investment Records published in the Internal Revenue Manual (IRM) 1.15.29 Submission Processing Campus Records.

- 42 – Internal Control Files: Destroy 1 year or when no longer needed in current operations

- 44 – Reference Files: Destroy when obsolete or superseded, or when no longer needed in current operations

- 49 – All Taxpayer Case Files: Destroy 3 years after case is closed or when no longer needed, whichever is earlier

- 101 – Unpostable and Nullified Unpostable Listing: Destroy 3 years after end of processing year in which closed or when no longer needed for internal audit, whichever is earlier

- 104 – Cycle Block Proof Listing: Destroy 1 year after end of processing year

- 105 – Notice Registers: (3) Output of Notice Correction - (a) Destruction criterion Destroy 1 year after end of processing year

- 165 – Revenue General Ledgers: (b) Destruction criterion - Destroy 6 years, 3 months after the period of the account

- 166 – Revenue Reports and Accounting Control Records: (1) Official File copy (a) Destruction criterion - Destroy after audit by General Accountability Office or when 3 years old, whichever is earlier

- 173 – Unit Ledger Cards: (1) (a)(b) Account Cards closed (Paid in Full, Abated, and Small Debit Write-Offs); All Other Account Cards closed due to Collection Statute Expiration Date (CSED) Destroy 20 years after end of processing year

- 174 – Accounting Reports: (1) Record Copy - (b) Destruction criterion - Destroy 3 years after end of reporting year

- 178 – (a) Destruction criterion Historic Transcripts related to closed accounts: Destroy 5 years after end of processing year.

14. Will this system use technology in a new way?
No. The system will not use technology in a new way.

15. Will this system be used to identify or locate individuals or groups? If so, describe the business purpose for this capability.
No. This system will not be used to identify or locate individuals or groups.

16. Will this system provide the capability to monitor individuals or groups? If yes, describe the business purpose for this capability and the controls established to prevent unauthorized monitoring.
No. This system will not provide the capability to monitor individuals or groups

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?
No. The system cannot allow IRS to treat taxpayers, employees, or others differently.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?
Yes. Upon receipt of a notice, the taxpayer has the right to contact taxpayer service for assistance for “due process”.

19. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors?
Yes, the system is web-based. However, persistent cookies are not used to identify web visitors.

View other PIAs on IRS.gov