Date of Approval: February 14, 2018 PIA ID Number: **3213**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Automated Non Master File (ANMF), ANMF

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.

ANMF, PIAMS #1250

Next, enter the **date** of the most recent PIA. 4/16/2015

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

No	Addition of PII
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
Yes	Internal Flow or Collection

Were there other system changes not listed above? No

If yes, explain what changes were made.

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
No	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.

The Automated Non-Master File (ANMF) supports accounting for assessment, liabilities, payments, and credits for transactions not compatible with master file processing, timeliness, or data. ANMF tracks receivables from taxpayers for Non-Master File (NMF) assessments, and generates billing notices to the taxpayers. The ANMF application consists of an electronic database that sends updated taxpayer data to the following systems: • Automated Lien System (ALS) • Financial Management Information System (FMIS) • Collection Statute Expiration Date (CSED) (Subsystem of Collection Activity Reports/Statutory Reports (CAR/SR) ANMF application sends summary data to the following system: • Redesign Revenue Accounting Control System (RRACS) formerly known as Interim Revenue Accounting Control System (IRACS) ANMF also prepares statistical data (non-taxpayer data) that is retrieved by the following system: • Enforcement Revenue Information System (ERIS) ANMF also prepares a tracking file (non-taxpayer data), that is retrieved by the following system: • Service Center Control File (SCCF) Data contained in ANMF for each taxpayer includes the individual and/or business taxpayer's name, Social Security Number (SSN), Employee Identification Number (EIN) or other Taxpayer Identification Number (TIN), individual and/or business address, and IRS accounts receivable and payable data. NMF data entry users use the ANMF system to enter key information from returns and related tax processing documents, and then formats it for computer processing. Original entry, key verification, and on-line error, blocks-out-of-balance, and non-postable corrections are used to perfect the data. The system standardizes the computation of interest and penalty reflected on taxpayer bills. NMF users have sole access for posting taxpayer information to the system, but the application is also accessible to the Revenue Accounting Control System (RACS) users for block control input and journal update. Other IRS functions are restricted to research capability. Reports generated from the ANMF database are for IRS internal use only, and are disseminated only to those with an authorized need to know and system authorization. Transcripts of the taxpayer's accounts developed in ANMF are provided to NMF within 24 hours of request.

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.

Yes On Primary Yes On Spouse No On Dependent

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

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

There is no known mitigation strategy planned to eliminate the use of SSN for the system; SSN is required for the use of this system. It is the main identifier for each record as it is the

tied to taxpayer information. The Office of Management and Budget Circular A-130 requires that federal agencies develop a mitigation or elimination strategy for systems that use SSNs, which the Service continues to develop strategies to meet. An exception to that requirement is when the SSN is uniquely needed to identify a user's record. The ANMF system requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer for intergovernmental communications. There is no known mitigation strategy planned to eliminate the use of SSNs for the system. The SSN is required for the use of this system. The SSN number is needed to research and locate records in response to the request.

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	No
Yes	Mailing address	No	No	No
No	Phone Numbers	No	No	No
No	E-mail Address	No	No	No
No	Date of Birth	No	No	No
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
No	Employment (HR) Information	No	No	No
Yes	Tax Account Information	Yes	Yes	Yes

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
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)	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.
Yes	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
Yes	Physical Security Information	Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities
Yes	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? No

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)
Yes	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.

The ANMF system tracks receivables from taxpayers for Non-Master File (NMF) assessments and generates billing notices to the taxpayers. ANMF supports accounting for assessment, liabilities, payments, and credits for transactions not compatible with master file processing, timeliness or data.

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

Data is original input and key verified by two separate operators to verify accuracy. System checks exist for validation of data. Each night, transactions input are systemically balanced to the Form 813, Block Control File, by Document Locator Number (DLN), debit and credit amount, and item count. The Data Manager runs the programs to balance all daily assessments to the Form 813, Block Control File. The NMF Error Register Listing is generated when the DLN of the input transaction does not match the DLN on the Block Control File. The Block Out of Balance (BOB) Summary is generated when the input transactions and Block Control File match on DLN but the item count or debit and credit amounts do not match. Separate Error Register and BOB Summary listings are generated from the Block Balance program for daily and weekly assessments. The subsequent transactions are included with the weekly assessments. Subsequent transactions and transactions input with Original Assessments are posted to the taxpayer's entity. Certain conditions will cause a transaction to unpost. These unpostable transactions are shown on the NMF Unpostable Transaction List. Each item on the unpostable list will have corresponding unpostable code (UPC). The NMF Unpostable List is generated and used to research and correct the unpostable transactions.

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? Yes

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

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

SORNS Number	SORNS Name
Treasury/IRS 22.060	Automated Non-Master File (ANMF)
Treasury/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. ##Official Use Only

E. INCOMING PII INTERFACES

11. Does the system receive SBU/PII from other system or agencies? 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
Automated Lien System (ALS)	Yes	01/16/2016	Yes	10/20/2015
Enforcement Revenue Information System (ERIS)	Yes	03/31/2015	Yes	07/17/2014
Financial Management Information System (FMIS)	Yes	10/05/2017	Yes	10/27/2017
Redesign Revenue Accounting Control System (RRACS)	Yes	05/05/2016	Yes	08/12/2015
Collection Statute Expiration Date (CSED - inactive)	No		No	08/12/2015
1099Pro (software)	No		No	08/12/2015

Identify the authority and for what purpose? The ANMF system tracks receivables from taxpayers for Non-Master File (NMF) assessments and generates billing notices to the taxpayers. ANMF supports accounting for assessment, liabilities, payments, and credits for transactions not compatible with master file processing, timeliness or data. The Authority is identified as: Title 26 of the Internal Revenue Code (IRC).

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, 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?
Automated Non-Master File (ANMF) tracks receivables from taxpayers for Non-Master File (NMF) assessments and generates billing notices to the taxpayers. ANMF supports accounting for assessment, liabilities, payments, and credits for transactions not compatible with master file processing, timeliness or data. Notice, consent and due process are provided via the IRS systems and their related tax forms instructions, and 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 Automated Non-Master File (ANMF) supports accounting for assessment, liabilities, payments, and credits for transactions not compatible with master file processing, timeliness, or data. ANMF tracks receivables from taxpayers for Non-Master File (NMF) assessments, and generates billing notices to the taxpayers using the taxpayers EIN or SSN. Notice, consent and due process are provided via the IRS systems and their related tax forms instructions, and pursuant to 5 USC.

19. How does the system or business process ensure due process regarding information access, correction and redress?
Upon receipt of a notice, the taxpayer has the right to contact taxpayer service for assistance for "due process". Notice, consent and due process are provided via the IRS systems and their related tax forms instructions, and pursuant to 5 USC.

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 and Write
Managers	Yes	Read-Only
Sys. Administrators	No	
Developers	No	

Contractor Employees? No

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

21a. How is access to SBU/PII determined and by whom? The user must submit an Online5081 to request access to ANMF which requires his/her manager's approval. Once approved by the manager, the HQ ANMF Analyst will review the request and add them to the 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? Not applicable

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.

ANMF master data files are approved for destruction when 1 year old or when no longer needed for administrative, legal, audit or other operational purposes (Job No. N1-58-97-13), as published under RCS 32, item 11 Records Control Schedule for Electronic Tax Administration. All procedures for eliminating the data at the end of the retention period are consistent with dispositions approved for specific recordkeeping copies of Wage and Investment covered under IRM 1.15.29, Records Control Schedule for Service Center Operations: • Item 42 – Internal Control Files: Destroy 1 year or when no longer needed in current operations • Item 44 – Reference Files: Destroy when obsolete or superseded, or when no longer needed in current operations • Item 49 – All Taxpayer Case Files: Destroy 3 years after case is closed or when no longer needed, whichever is earlier • Item 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 • Item 104 – Cycle Block Proof Listing: Destroy 1 year after end of processing year • Item 105 – Notice Registers: (3) Output of Notice Correction – (a) Destruction criterion Destroy 1 year after end of processing year • Item 165 – revenue General Ledgers: (B) Destruction criterion – Destroy

6 years, 3 months after the period of the account • Item 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 • Item 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 • Item 174 – Accounting Reports: (1) record Copy – (b) Destruction criterion – Destroy 3 years after end of reporting year • Item 178 – (a) Destruction criterion Historic Transcripts related to closed accounts: Destroy 5 years after end of processing year.

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? 8/28/2017

23.1 Describe in detail the systems audit trail. The following data elements are collected in the ANMF audit trail at the system level: User Login/Logout time is recorded, including date, time, and associated User ID. At the application level, the following data fields are captured in the application's history file: Date and identity of who created and/or last modified the data in each table, list or report. The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies the necessary IRS personnel. ANMF 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

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?
A system POA&M has been made and is being monitored with milestones and quarterly updates. Treasury FISMA Inventory Management System (TFIMS) shows the most recent update on the finding: 11/01/2014 - The progress of this finding has not been something that the application can fix on its own. This finding might extend past the Plans Of Action & Milestones (POA&M's) due date. Please keep in mind...ANMF developers are not directly responsible for implementing this.

24b.1. If **completed**, where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)? They system was tested between 6/21/2017- 8/28/2017. The results of the testing are housed in the Treasury FISMA Inventory Management System (TFIMS) repository. Confirmation that requirements have been met were confirmed with the issuance of the Assessment final package which included the test results in an assessment plan, and documented in the Security Assessment Report(SAR).

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? No

L. NUMBER AND CATEGORY OF PII RECORDS

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

26a. IRS Employees: Under 50,000
26b. Contractors: Under 5,000
26c. Members of the Public: Under 100,000
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