Date of Approval: January 18, 2018 PIA ID Number: **3184**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Account Management Services, AMS

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.

Account Management Services, AMS, 2834

Next, enter the **date** of the most recent PIA. 9/26/2017

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
No	Internal Flow or Collection

Were there other system changes not listed above? Yes

If yes, explain what changes were made. The AMS PCLIA is being updated to revise the Authorizing Official (AO) and Subject Matter Expert (SME) information.

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 scope of the Account Management Services (AMS) project is to provide Internal Revenue Service (IRS) employees with applications enabling on-demand user access and management of taxpayer accounts. IRS' account management process spans the lifecycle of a taxpayer account, from establishment of a new account, through periodic updates, posting of payments, reconciliation of deposits, account adjustments, and settlements. As the IRS modernizes its business processes and Information Technology (IT) infrastructure, the ability to provide immediate access to integrated account data, enable real-time transaction processing, and settle accounts on a daily basis is recognized as critical to achieving improved business results, including improved customer service.

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 Yes 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)
Yes 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).

AMS requires the use of a Taxpayer Identification Number (TIN) or a unique identifier listed on an IRS issued notice; letter; or taxpayer initiated correspondence or telephone call to access the taxpayer's account information listed in the AMS application. The AMS application participated in the Social Security Number (SSN) 2-D bar code pilot that began in July 2011. The Office of Privacy, Governmental Liaison and Disclosure (PGLD) has oversight of the 2-D bar code pilot. It is anticipated the PGLD office will incorporate additional notices into the 2-D bar code project in the future. AMS will coordinate with the PGLD office to incorporate additional notices into the 2-D bar code project when PGLD deems it necessary.

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
Yes	Phone Numbers	No	No	No
Yes	E-mail Address	No	No	No
Yes	Date of Birth	Yes	Yes	Yes
No	Place of Birth	No	No	No
Yes	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
Yes	Vehicle Identifiers	No	No	No
No	Passport Number	No	No	No
No	Alien (A-) Number	No	No	No
Yes	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.
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? Yes

If **yes**, describe the other types of SBU/PII that are applicable to this system. Power of Attorney (POA).: name, address, telephone number, userid (User Identification), Centralized Authorization File (CAF), business address, business name, city, state, zip code, e-mail address; Tax Practitioner: Name and address; Reporting Agent File (RAF): IRS Reporting Agent Name; Return Refund Check Processing System; Taxpayer Identification Number (TIN); Taxpayer Telephone number; Transcript data Taxpayer Address; Employer Identification Number (EIN); Module data: transaction record, tax period, received date for case; Issue codes: reason for filing the case, dollar amount owed, interest, penalty, payment amount, refund amount, balance due amount, history for taxpayer advocate services users only; Employer name; Employer address; Employer Telephone Number; Business Name and Address; Business Telephone Number; Correspondence Information (Type of correspondence and date); History Information (Type of contact, resolution of address change and date); Financial Information (Bank name/address/telephone number, routing number, name of the account holder, account number, real estate, assets, wage and levy sources); Type of Tax, (e.g. Form 1040; Form 941; etc.); Filing Status; Business Operating Indicator; Entity data (i.e., taxpayer name, Tax Identification Number (TIN), address, date of birth (DOB), filing status, home phone number, business phone number); Process codes; Adjusted gross income (AGI); Itemized deductions or standard deductions; Taxable income; Affordable Care Act (ACA) Exemption Number; ACA Policy Number; and ACA Exemption Certificate Number (ECN)

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.

IRS employees use the AMS application to assist taxpayers with tax account services and tax compliance matters. Taxpayer Identification Numbers are required to provide this service. The scope of the Account Management Services (AMS) project is to provide IRS employees with applications enabling on-demand user access and management of taxpayer accounts. IRS'

account management process spans the lifecycle of a taxpayer account, from establishment of a new account, through periodic updates, posting of payments, reconciliation of deposits, account adjustments, and settlements.

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

AMS does not collect data from other outside sources other than IRS records. AMS provides several validity checks on data that is entered into the system. Each set of data that is required is checked for the validity of each and every data item to ensure that all the required data is entered correctly. Additionally, AMS provides validation of information entered into the system by displaying screen indicators to notify the user that more information is necessary or data is entered incorrectly. For example, when the taxpayer information is entered, (i.e., name, address) AMS systemically checks for valid character and numeric data when displaying and during input.

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

SORNS Number	SORNS Name
Treasury/IRS 24.046	CADE Business Master File
Treasury/IRS 34.037	IRS Audit Trail and Security Records System
Treasury/IRS 00.001	Correspondence Files
Treasury/IRS 24.030	CADE Individual Master File

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. ## For official Use Only

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
Automated Collection System (ACS)	Yes	12/18/2015	Yes	02/05/2015
Integrated Data Retrieval System (IDRS)	Yes	08/29/2017	Yes	12/21/2016
Automated Trust Fund Recovery Program (ATFR)	Yes	02/12/2017	Yes	05/31/2017
Online 5081 (OL5081)	Yes	08/04/2015	Yes	06/15/2015

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

If **yes**, identify the source that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

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
On-Line 5081 (OL5081)	Yes	08/04/2015	Yes	06/15/2015
Taxpayer Advocate Management Information System (TAMIS)	Yes	06/05/2017	Yes	03/30/2017
Integrated Data Retrieval System (IDRS)	Yes	08/29/2017	Yes	12/21/2016
Compliance Data Warehouse (CDW)	Yes	03/18/2016	Yes	02/11/2015
Automated Collection System (ACS)	Yes	12/18/2015	Yes	02/05/2015
Automated Underreporter (AUR)	Yes	06/06/2016	Yes	12/28/2015
Automated Trust Fund Recovery (ATFR)	Yes	02/12/2017	Yes	05/31/2017

Identify the authority and for what purpose? AMS collects information from and disseminates information to IRS systems for the purposes of tax administration under Internal Revenue Code Sections 6001, 6011, 6012e(a). Internal Revenue Code Section 6109 authorizes the collection and use of SSN information.

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?
The AMS system receives data from other IRS upstream sources/systems. Those other sources/systems provide the Privacy Act Notice to individuals/businesses. 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? Yes

18a. If **yes**, describe the mechanism by which individuals indicate their consent choice(s):
The AMS system receives data from other IRS upstream sources/systems. Those other sources/systems provide the Privacy Act Notice to individuals/businesses. 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?
The AMS system receives data from other IRS upstream sources/systems. Those other sources/systems provide the Privacy Act Notice to individuals/businesses. 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 and Write
Sys. Administrators	Yes	Read and Write
Developers	Yes	Read-Only

Contractor Employees? Yes

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

21a. How is access to SBU/PII determined and by whom? Online 5081 (OL5081) is used to document access requests, modifications and terminations for all types of users, including system administrators, system accounts, and test accounts. A new user needs to request access for a system or application via OL5081. OL5081 will then notify the manager of the request and the manager will then approve the request via OL5081. The completed OL5081 is submitted to the account administration approval group, who assigns a user ID (User Identification) and an initial password. Before access is granted, the user is required to digitally sign OL5081 acknowledging his/her security responsibilities when using the system. The user signs security rules of behavior provided in the OL5081. Employees will have access to accounts assigned to them and accounts necessary to perform their official duties. Pursuant to the rules described in UNAX (Unauthorized Access of Taxpayer Accounts), employees are not allowed to access their own accounts, their spouses account and immediate family member's account. Third-party providers (i.e., contractors) for the AMS application are subjected to the same application system policies and procedures of the IRS as employees. Additionally, contractors must conform to the same security controls and documentation requirements that would apply to the organization's internal systems; which are enforced through the appropriate Contracting Officer's Representative (COR). IRS and contractor employees must successfully pass Personnel Screening and Investigation, (PS&I), appropriate to their need and be trained on Internal Revenue Service (IRS) security and privacy policies and procedures, including the consequences for violations. Logons and user profiles will be used to ensure the integrity of the AMS System and the AMS Program.

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.

All records housed in the AMS system will be erased or purged from the system in accordance with approved retention periods. It is the official repository for data and documents and has National Archives approval to affect data disposition. Any records generated and maintained by the system will be managed according to requirements under IRM 1.15.1 and 1.15.6, and will be destroyed using IRS Records Control Schedule (RCS) 29, Item 425 and as coordinated with the IRS Records and Information Management (RIM) Program and IRS Records Officer. AMS master data files are approved for destruction 2 years after last account access to taxpayer record (Job No. N1-58-09-59, approved 5/4/2010).

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? 4/3/2017

23.1 Describe in detail the system s audit trail. Employee SEID (Standard Employee Identifier) ; Employee name; Date of action; Activity; Taxpayer Tax Identification Number (TIN); Type of event, including logon and logoff, opening and closing of files, stored and ad hoc queries, and all actions by System Administrators (SAs); Role of user creating event; Success or failure of the event; Terminal Identification (ID); IDRS employee ID; Time of action; Master file tax code (MFT), tax period; Type of contact AMS keeps a history of specific actions taken by the employee with regards to a specific taxpayer. This history contains entries that are created automatically and entries that can be created at any time by the employee to document the steps taken with respect to the taxpayer's data.

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?
There is no use of live data during the development testing phase of the AMS system changes. Privacy Requirements were met when the system was established and granted an Authorization to Operate (ATO). The AMS Application interfaces protect PII in transit through the use of Enterprise File Transfer Utility (EFTU); access control, audit and encryption capabilities. Additionally, AMS operates using IRS infrastructure and behind the IRS firewall.

24b.1. If **completed**, where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)? Doc IT

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
If **no**, explain why not.

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: 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