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: November 6, 2014 PIA ID Number: **1066**

1. What type of system is this? Modernized System

1a. Is this a Federal Information Security Management Act (FISMA) reportable system? Yes

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

Account Management Services, AMS

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:	Over 1,000,000

4. Responsible Parties:

NA

5. General Business Purpose of System

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. 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.

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: 4/19/2012 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

COTs Upgrades version updates. Interface between AMS and the Enterprise Service Bus (ESB) - This supports the expansion of AMS for the implementation of the Affordable Care Act (ACA) AMS uses web services provided by ACA to interface with related systems such as Coverage Data Repository (CDR) and ACA Verification Service (AVS) for data retrieval and PTC calculations.

7. If this system has an Exhibit 53 or Exhibit 300 please provide the Unique Project Identifier (UPI) number (XXX-XX-XX-XX-XX-XXXX-XX). Otherwise, enter the word 'none' or 'NA'. 015-45-01-14-01-2463-00

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	Yes	
Other	Yes	*Other Source:* Automated Collection System (ACS)

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	Yes
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

PII Name	On Public?	On Employee?
ACA Exemption number	Yes	No
ACA Policy Number	Yes	No
ACA Exemption Certificate Number (ECN)	Yes	No

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

AMS collects and uses Taxpayers SSNs to assist taxpayers in servicing and settling their tax accounts.

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.)

The regulations/internal revenue codes that deal specifically with requiring taxpayers to provide their SSN or EIN to IRS are: IRC 6011; IRC 6109-1; 26 CFR Section 301.6109-1 6011 requires the return, and 6109-1 says you have to provide an SSN if you're required to file a return.

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

The AMS application participated in the 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.

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

AMS will coordinate with the PGLD office to incorporate additional notices into the 2-D bar code project when PGLD deems it necessary.

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

Power of Attorney (POA).: name, address, phone number, userid, Centralized Authorization File (CAF), business address, business name, city, state, zip, 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, TIN, address, date of birth (DOB) filing status, home phone number, business phone number); Process codes; Adjusted gross income; Itemized deductions or standard deductions; Taxable income

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.

Employee SEID; Employee name; Date of action; Activity; Taxpayer TIN; Type of event, including logon and logoff, opening and closing of files, stored and ad hoc queries, and all actions by System Administrators; Role of user creating event; Success or failure of the event; Terminal 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.

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:

System Name	Current PIA?	PIA Approval Date	SA & A?	Authorization Date
ACA Verification Service (AVS) - Component of ACA IS	Yes	04/16/2013	Yes	02/27/2014
Coverage Data Repository (CDR) - Component of ACA IS	Yes	04/16/2013	Yes	02/27/2014
Online 5081 (OL5081)	Yes	07/17/2012	Yes	08/29/2012
Taxpayer Advocate Management Information System (TAMIS)	Yes	02/17/2012	Yes	06/07/2012
Automated Collection System (ACS)	Yes	12/11/2012	Yes	04/23/3013
Automated Underreporter (AUR)	Yes	07/12/2013	Yes	10/01/2014
Automated Trust Fund Recovery Program (ATFR)	Yes	02/10/2014	Yes	06/10/2014
Compliance Data Warehouse (CDW)	Yes	12/14/2012	Yes	01/24/2012
Integrated Data Retrieval System (IDRS)	Yes	08/03/2014	Yes	12/09/2011

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): Yes

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.

IRS employees use the AMS application to assist taxpayers with tax account services and tax compliance matters.

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	Yes	
To provide taxpayer services	Yes	
To collect demographic data	No	
For employee purposes	No	
		If other, what is the use?
Other:	No	

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		
		If other, specify:
Other:		

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

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	No
Website Opt In or Out option	No
Published System of Records Notice in the Federal Register	No
Other: The data in this application comes from other IRS systems.	Yes

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:	Yes	
Users		Read Write
Managers		Read Write
System Administrators		Read Write
Developers		No Access
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?

Online 5081 (OL5081) is used to document access requests, modifications and terminations for all types of users, including system administrators, system accounts requiring File Transfer Protocol (FTP) access, 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 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, 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 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.

---

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

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.

---

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.

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). These disposition instructions are published in Records Control Schedule (RCS) Document 12990 under RCS 29 for Submission Processing Campus Records, Item 425.

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.

Pursuant to the rules described in UNAX, employees are not allowed to access their own accounts, their spouses account and immediate family member's account. Prior to processing a TIN request, an IDRS request is first validated against Security and Communication Systems (SACS) to ensure conformance with UNAX policy. If the TIN entered violates UNAX policy (i.e., employees own TIN, spouses, or immediate family member), then the employee will be reprimanded and/or prosecuted. All IRS rules and regulations against browsing and unauthorized access will be reemphasized and monitored. Procedures are in place to deter and detect browsing and unauthorized access prescribed by UNAX policy. AMS personnel will ensure that: (1) records or documents show that the organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions; (2) (i) - Audit trails shall be used to review what occurred after an event and for real-time analysis. A systemic query will be run against the data and a report generated to identify suspicious activity and this report will be provided to management. (ii) - Security Specialists shall be assigned the responsibility to review audit information including the following: (a) Audit trail review after an event; and (b) Scheduled audit reviews listed in the AMS ESAT approved audit plan. (iii) - Audit tools shall allow management to hold employees accountable for user actions on computer systems. Access to on-line audit logs is strictly controlled. Audit logs are protected by strong access controls to help prevent unauthorized access to ensure events are not overwritten. The archived audit records only have read authority granted. Additionally, there is a list of TIN summary reports generated for managerial review, and a systemic negative TIN check that is performed by SACS that indicates if an employee accesses their own, spouses or immediate family member accounts. If so, appropriate disciplinary actions are taken. In addition, these reports are also sent to SAAS audit monitoring system.

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

Pursuant to the rules described in UNAX, employees are not allowed to access their own accounts, their spouses account and immediate family member's account. Prior to processing a TIN request, an IDRS request is first validated against Security and Communication Systems (SACS) to ensure conformance with UNAX policy. If the TIN entered violates UNAX policy (i.e., employees own TIN, spouses, or immediate family member), then the employee will be reprimanded and/or prosecuted. All IRS rules and regulations against browsing and unauthorized access will be reemphasized and monitored. Procedures are in place to deter and detect browsing and unauthorized access prescribed by UNAX policy. AMS personnel will ensure that: (1) records or documents show that the organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions; (2) (i) - Audit trails shall be used to review what occurred after an event and for real-time analysis. A systemic query will be run against the data and a report generated to identify suspicious activity and this report will be provided to management. (ii) - Security Specialists shall be assigned the responsibility to review audit information including the following: (a) Audit trail review after an event; and (b) Scheduled audit reviews listed in the AMS ESAT approved audit plan. (iii) - Audit tools shall allow management to hold employees accountable for user actions on computer systems. Access to on-line audit logs is strictly controlled. Audit logs are protected by strong access controls to help prevent unauthorized access to ensure events are not overwritten. The archived audit records only have read authority granted. Additionally, there is a list of TIN summary reports generated for managerial review, and a systemic negative TIN check that is performed by SACS that indicates if an employee accesses their own, spouses or immediate family member accounts. If so, appropriate disciplinary actions are taken. In addition, these reports are also sent to SAAS audit monitoring system.

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? Yes

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

Testing is conducted annually to ensure the selected controls are functioning correctly. When testing of a security control reveals that the control is not functioning as expected, the control deficiency is documented in the system's plan of action and milestones (POA&M). All test results are documented and reported to Business Unit (BU) Security Project Management Office (SPMO). The security state of the application is then reported to the appropriate organizational officials annually as defined in Treasury Directives Policy (TDP) 85-01.

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:

N/A