Account Management Services (AMS) – Release 2.1, Milestone 5, Version 1.0
Privacy Impact Assessment (PIA)

PIA Approval Date: November 10, 2009

System Overview

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's 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.

Data in the System

1. Generally describe the information to be used in the system in each of the following categories: Taxpayer, Employee, and Other.

Taxpayer: AMS stores or displays the following information on the taxpayer:

- Taxpayer Identification Number (TIN)
- Phone number
- Transcript data
- TIN Type
- Taxpayer name
- 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
- Business Name and Address
- Correspondence Information (Type of correspondence and date)
- History Information (Type of contact, resolution of address change and date)
- Financial Information (Bank name and address, routing number, name of the account holder, account number, real estate, assets, wage and levy sources)
- Type of Tax, (e.g. Form 1040)
- 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

Employee: AMS will collect the following information during the course of the employees use of AMS and to determine the employee's access to the application. AMS stores the following information on the employee.

- Standard Employee Identifier (SEID): when the employee logs onto the work station, the system attempts to match the SEID entered. If the there is a match, the employee can proceed
- Employee name
- Organization
- Work Phone Number
- User Identification
- Role designation: System Administrator (SA), Manager, Customer Service Representative (CSR), System Security Administrator (SSA)
- IDRS employee number
- Mail Stop
- Skill sets

Audit Trail Information: AMS utilizes IDRS Audit log for all IDRS Commands issued via AMS and sends Logs to SAAS as Required. AMS's internal audit log consists of the:

- 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.

Other:

- 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

2. What are the sources of the information in the system?
AMS will store information on the taxpayer received from the below systems:

- Integrated Data Retrieval System (IDRS): TIN, taxpayer name, address, phone number
- Individual Master File (IMF) and Business Master File (BMF): transcript data
- Electronic Account Resolution (EAR**):** TIN

AMS will display taxpayer information received from the below systems:

- Automated Underreporter (AUR): CP2000 Form, process codes, correspondence history
- Integrated Data Retrieval System (IDRS): TIN, taxpayer name, address, phone number
- IMF and BMF (transcript data)
- Non MasterFile (NMF): TIN, taxpayer name, address, module data (transaction record, tax period)
- Taxpayer Advocate Management Information System (TAMIS): Taxpayer name, received date for cases, issue codes(reason for filing the case) tax period, dollar amount owed, refund amount, balance due amount, history for taxpayer advocate services users only.
- Electronic Account Resolution (EAR): TIN, Power of Attorney (POA): name, address, phone number, userid, Centralized Authorization File (CAF), business address, business name, city, state, zip, e-mail address
- Corporate Files On-Line (CFOL): TIN, name, address, phone number

*AMS does not receive employee information from the above systems.

2.a. What IRS files and databases are used?
IRS files and databases used are: IMF, CFOL, IDRS, EAR (reporting information), BMF, NMF, AUR, TAMIS

2.b. What Federal Agencies are providing data for use in the system?
Federal Agencies are not providing data for use in the system.

2.c. What State and Local Agencies are providing data for use in the system?
State or local agencies are not providing data for use in the system.

2.d. From what other third party sources will data be collected?
Taxpayer information will be collected from the Power of Attorney, Tax Practitioner, and Reporting Agent all via EAR.

2.e. What information will be collected from the taxpayer/employee?

Taxpayer: AMS will collect, display and store the following information from the taxpayer:

- TIN
- Transcript data
- Taxpayer name
- Taxpayer Address

- Phone number
- Module data: transaction record, tax period, received date for case
- Issue codes: reason for filing the case, tax period, dollar amount owed, interest, penalty, payment amount, refund amount, balance due amount, history for taxpayer advocate services users only.

Employee: Data which will be collected from employees during authentication includes:

- SEID
- Employee name
- Organization
- Work Phone Number
- User Identification
- Role designation: SA, Manager, CSR, SSA
- IDRS employee number

3.a. How will the data collected from sources other than IRS records and the taxpayers be verified for accuracy?
AMS does not collect data from other outside sources other than IRS records. AMS receives the information that the Tax Practitioner provides from EAR.

3.b. How will data be checked for completeness?
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.

3.c. Is the data current? How do you know?
Yes. There is a day-time-stamp for data stored in AMS. AMS relies on data transferred from other systems to AMS to be current.

4. Are the data elements described in detail and documented? If yes, what is the name of the document?
The Business System Requirement Report, the Business Architectural Report, the Design Specification Report (DSR) and Interface Control Documents (ICD) will provide a detailed description of the data elements. These documents are for internal use only and are not made accessible to the public.

<u>Access to the Data</u>

1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?

- **Users:** IRS employees have been granted access to the system as necessary to fulfill their duties according to their role. Currently, approximately 34,000 internal customer users (Users and Managers) have access to the taxpayer data. AMS is accessed via a standard web browser (e.g., Internet Explorer). The primary users will be Wage & Investment (W&I) users. Secondary users are from Small Business/Self-Employed (SB/SE), Taxpayer Advocate, and Appeals. Access to the data is determined by the manager based on a user's position, job

duties and need-to-know.

- **Managers/Acting Manager:** Access similar to the Users, with the added capability to manage those Users who are profiled within the Manager's group.

- **System Security Administrators (SSA):** Only has access to the user profile. SSAs do not have access to the standard functionality within AMS. SSAs only have access to those functions that relate to the maintenance of the application, including, but not limited to, adding Users, moving Users and changing a User status.

- **System Administrators/Database Administrators (SA, DBA):** SA's and DBA's are IRS employees with necessary access to provide SA and DBA support for AMS supported hardware.

2. How is access to the data by a user determined?
Online 5081 is used to document access requests, modifications and terminations for all types of users, including system administrators, system accounts requiring 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 Technical Representative (COTR).

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.

2. a. Are criteria, procedures, controls, and responsibilities regarding access documented?
Yes. 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 can be written up or prosecuted.

3. Will users have access to all data on the system or will the user's access be restricted? Explain.
Pursuant to the rules described by UNAX, employees are not allowed to access their own accounts, their spouses account and immediate family member's account. Employees will have access to accounts assigned to them and accounts necessary to perform their official duties. Access to individuals' case inventory is restricted to a role-based limitation. For example, a CSR cannot view

the contents of another CSR's inventory, but a manager can have access to an employee's inventory below him/her. Although one user can occupy multiple roles within the software application, a user cannot be assigned as his/her own manager or work leader.

4. What controls are in place to prevent the misuse (e.g. browsing) of data by those having access?
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 (refer to question 2a).

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 at least weekly or more frequently at the discretion of the information system owner. (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.

5.a. Do other systems share data or have access to data in this system? If yes, explain.
Yes. The following systems share data with AMS:

- Integrated Data Retrieval System: TIN, taxpayer name, address, phone number
- Individual Master File and Business Master File: transcript data
- Automated Underreporter: CP2000 Form, process codes, correspondence history
- Non MasterFile: TIN, taxpayer name, address, module data (transaction record, tax period)
- Taxpayer Advocate Management Information System: Taxpayer name, received date for cases, issue codes(reason for filing the case) tax period, dollar amount owed, refund amount, balance due amount, history for taxpayer advocate services users only.
- Electronic Account Resolution: TIN, Power of Attorney (POA): name, address, phone number, userid, Centralized Authorization File (CAF), business address, business name, city, state, zip, e-mail address
- Corporate Files On-Line: TIN, name, address, phone number

There are no systems that have access to data in the AMS system.

5.b. Who will be responsible for protecting the privacy rights of the taxpayers and employees affected by the interface?
The Business Owner is responsible for protecting the privacy rights of the taxpayers and employees.

6.a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, & Other)?
No other International, Federal, State, or Local agencies will share data or have access to data in this system.

6.b. How will the data be used by the agency?
N/A

6.c. Who is responsible for assuring proper use of the data?
N/A

6.d. How will the system ensure that agencies only get the information they are entitled to under IRC 6103?
N/A

Attributes of the Data

1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?
Yes. The use of the following data in the IRS databases is both relevant and necessary in order to resolve taxpayer issues. The data in IDRS enables users to identity taxpayer TIN, which is necessary to access the taxpayer's account via AMS or the system that interfaces with AMS. The taxpayer address and name allow users to resolve a taxpayer inquiry. EAR data is necessary to reconstruct the EAR inventory record and display it to the user. For all other systems that store or display the below data in AMS, it is used to validate taxpayer requirements:

Taxpayer:

- Taxpayer Identification Number (TIN)
- Phone number
- Transcript data
- TIN Type
- Taxpayer name
- Taxpayer Address
- 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
- Business Name and Address
- Correspondence Information (Type of correspondence and date)
- History Information (Type of contact, resolution of address change and date)
- Financial Information (Bank name and address, routing number, name of the account holder, account number, real estate, assets, wage and levy sources)
- Type of Tax, (e.g. Form 1040)

- 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
- Employee Identification number EIN

Employee:

- SEID: when the employee logs onto the work station, the system attempts to match the SEID entered. If the there is a match, the employee can proceed.
- Employee name
- Organization
- Work Phone Number
- User Identification
- Role designation: SA, Manager, CSR, SSA
- IDRS employee number
- Date of action Activity
- IDRS employee number
- Mail Stop
- Skill sets

2.a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

- **Taxpayer:** No. The data that is transferred and or input into AMS is stored upon receipt and not modified

- **Employee:** No. The data that is transferred and or input into AMS is stored upon receipt and not modified.

2.b. Will the new data be placed in the individual's record (taxpayer or employee)?

- **Taxpayer:** N/A

- **Employee:** N/A

2.c. Can the system make determinations about taxpayers or employees that would not be possible without the new data?

- **Taxpayer: N/A**

- **Employee: N/A**

2.d. How will the data be verified for relevance and accuracy?
The system does not derive new data, therefore, verification for relevancy is not applicable.

3.a. If the data is being consolidated, what controls are in place to protect the data and prevent unauthorized access? Explain.
For AMS Release 2.1, data will not be consolidated.

3.b. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.
For AMS Release 2.1, processes are not consolidated.

4. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.
For the AMS system, IRS employees retrieve taxpayer accounts only by the taxpayer's TIN and or Inventory Type. The employee data can only be retrieved by the employee's SEID, SSN and work group location. The Manager, Acting Manager and Frontline Manager assigned to the employee can look up the employee by name and the SSN can look up the employee by SEID, SSN and work group location.

5. What are the potential effects on the due process rights of taxpayers and employees of:

a. Consolidation and linkage of files and systems;
- **Taxpayer:** N/A. There is no consolidation and linkage of files and systems in this release.

- **Employee:** N/A. There is no consolidation and linkage of files and systems in this release.

b. Derivation of data;
- **Taxpayer:** No. The data that is transferred and or input into AMS is stored upon receipt and not modified. The Image File can update but not modify the case data.

- **Employee:** No. The data that is transferred and or input into AMS is stored upon receipt and not modified by authorized users. The CSR can update the system with a name, phone number, location and mail stock number. A manager can modify the employees IDRS number.
  If the employee's IDRS number is modified, the employee will notice the change once the employee views his/her profile or if the IDRS number has been changed, it will prevent the employee from working cases and this will alert the employee that changes have been made to the employee's profile.

c. Accelerated information processing and decision making;
- **Taxpayer:** N/A. There is no acceleration of information processing and decision making in regards to taxpayer data.

- **Employee:** N/A There is no acceleration of information processing and decision making in regards to employee data

d. Use of new technologies;
- At this time, there are no new technologies being used for R2.1 MS 5

How are the effects to be mitigated?
- There is no impact on the due process rights of the employee and taxpayer.

Maintenance of Administrative Controls

1.a. Explain how the system and its use will ensure equitable treatment of taxpayers and employees.
AMS training will emphasize that all taxpayers are entitled to due process and all CSRs will have specific procedures for these situations. Additionally, taxpayers are notified of their right to seek assistance from Taxpayer Advocate Services (TAS).

1.b. If the system is operated in more than one site, how will consistent use of the system be maintained at all sites?
The system is centralized with remote Users. Remote Users can view the data in the system, but cannot download data to their workstation.

1.c. Explain any possibility of disparate treatment of individuals or groups.
None. The system has the capability to single out individual taxpayers; however, the AMS system does not provide disparate treatment to individuals or groups of taxpayers by providing special treatment, whether favorable or unfavorable.

2.a. What are the retention periods of data in this system?
For systems that store or process taxpayer information, audit trail archival logs are retained per IRM 1.15., Records Management-Types of Records and their Lifecycles.

2.b. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?
Records reposited in the AMS will be destroyed in compliance with records retention instructions authorized in the Records Control Schedules of the Internal Revenue Service (IRM 1.15.8 through IRM 1.15.29). The System houses and manages mixed series of records and will utilize the EMC Documentum Suite Records Management Application to affect authorized disposal according to the maximum retentions approved for each type of record.

2.c. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?
Data that is captured by AMS audit trails are a chronology of events. AMS relies on IRS databases for accuracy, relevancy, timeliness and completeness of the data in the system. When a case is active the CSR updates after case is closed

3.a Is the system using technologies in ways that the IRS has not previously employed (e.g. Caller-ID)?
No.

3.b How does the use of this technology affect taxpayer/employee privacy?
N/A

4.a Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.
Yes. The system provides the capability to identify, locate, and monitor employees and taxpayers through audit trails, case history, and case notes for the purpose of resolving taxpayer issues.

4.b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.
Yes. The system provides the capability to identify, locate, and monitor employees and taxpayers through audit trails, case history, and case notes for the purpose of resolving taxpayer issues and unauthorized access activity events..

4.c. What controls will be used to prevent unauthorized monitoring?
Pursuant to the rules described by Unauthorized Access (UNAX) and Negative TIN policy, employees are not allowed to access their own accounts, their spouses account and immediate family member's account. If so, appropriate disciplinary actions are taken.

5.a Under which Systems of Record Notice (SORN) does the system operate? Provide number and 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

5.b. If the system is being modified, will the SORN require amendment or revision? Explain
No. There is no new data being added for R2.1 according to SORN requirements.

View other PIAs on IRS.gov