Date of Approval: November 01, 2023

PIA ID Number: 8246

SYSTEM DESCRIPTION

Enter the full name and acronym for the system, project, application and/or database.

Account Management Services, AMS

Is this a new system?

No

Is there a PCLIA for this system?

Yes

What is the full name, acronym, and milestone of the most recent PCLIA?

Account Management Services, AMS, 5626

What is the approval date of the most recent PCLIA?

11/20/2020

Changes that occurred to require this update:

Expiring PCLIA

Were there other system changes not listed above?

No

What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym.

Compliance Governance Board

Current ELC (Enterprise Life Cycle) Milestones:

Operations & Maintenance (i.e. system is currently operational)

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

Yes

GENERAL BUSINESS PURPOSE

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.

PII DETAILS

Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information: or any other type of Sensitive but Unclassified (SBU) information or PII such as information about IRS employees or outside stakeholders?

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

What types of tax identification numbers (TIN) apply to this system?

Social Security Number (SSN)

List the approved Treasury uses of the SSN:

Legal/statutory basis (e.g. where collection is expressly required by statute)

When there is no reasonable alternative means for meeting business requirements

Another compelling reason for collecting the SSN

Explain why the authorized use(s) above support the new or continued use of SSNs (or tax identification numbers).

AMS requires the use of a Taxpayer Identification Number (TIN) 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. It is the only unique identifier associated with taxpayers, spouses, and dependents that can be used to ensure the correct records are accessed. In addition, the TIN is used to restrict access by complying with the Taxpayer Browsing Protections Act.

Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN's (or tax identification numbers).

The Office of Management and Budget (OMB) 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 SSN is the significant part of the data being processed/received/disseminated by AMS and required to identify an AMS record.

Does this system use, collect, receive, display, store, maintain or disseminate other (non-SSN) PII (i.e. names, addresses, etc.)?

Yes

Specify the PII Elements:

Name
Mailing address
Phone Numbers
E-mail Address
Date of Birth
Standard Employee Identifier (SEID)
Internet Protocol Address (IP Address)
Vehicle Identifiers
Financial Account Numbers
Employment Information
Tax Account Information
Centralized Authorization File (CAF)

Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?

Yes

Specify the types of SBU from the SBU Types List (SBUList):

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.

Are there other types of SBU/PII used in the system?

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)

Cite the authority for collecting SBU/PII (including SSN if relevant).

PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, & 6012e(a)

SSN for tax returns and return information is Internal Revenue Code Section 6109

BUSINESS NEEDS AND ACCURACY

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 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.

How is the SBU/PII verified for accuracy, timeliness, and completion?

AMS does not collect data from 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 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.

PRIVACY ACT AND SYSTEM OF RECORDS

The Privacy Act requires Federal agencies that maintain a system of records to publish systems of records notices (SORNs) in the Federal Register for records from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence. The Privacy Act also provides for criminal penalties for intentional noncompliance.

Does your application or this PCLIA system pertain to a group of any record from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence? An identifier may be a symbol, voiceprint, SEID, or other personal identifier that is used to retrieve information.

Yes

Identify the Privacy Act SORN(s) that cover these records.

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

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

INCOMING PII INTERFACES

Does the system receive SBU/PII from other systems or agencies?

Yes

Does the system receive SBU/PII from IRS files and databases?

Yes

Enter the files and databases:

System Name: Enterprise Application Integration Broker (EAIB) (Part of Enterprise System Domain (GSS-17))
Current PCLIA: Yes
Approval Date: 8/18/2021
SA&A: Yes
ATO/IATO Date: 8/28/2023

System Name: Taxpayer Advocate Management Inventory Service (TAMIS)
Current PCLIA: Yes
Approval Date: 6/2/2020
SA&A: Yes
ATO/IATO Date: 3/14/2020

System Name: Automated Collection System (ACS)
Current PCLIA: Yes
Approval Date: 10/1/2021
SA&A: Yes
ATO/IATO Date: 12/1/2021

System Name: Integrated Data Retrieval System (IDRS)
Current PCLIA: Yes
Approval Date: 10/26/2021
SA&A: Yes
ATO/IATO Date: 11/1/2021

System Name: Automated Trust Fund Recovery Program (ATFR)
Current PCLIA: Yes
Approval Date: 11/2/2022
SA&A: Yes
ATO/IATO Date: 6/14/2022

System Name: Business Entitlement Access Request System (BEARS)
Current PCLIA: Yes
Approval Date: 8/25/2021
SA&A: Yes
ATO/IATO Date: 4/20/2023

System Name: Affordable Care Act (ACA)
Current PCLIA: Yes
Approval Date: 5/7/2021
SA&A: Yes
ATO/IATO Date: 12/5/2022

Does the system receive SBU/PII from other federal agency or agencies?

No

Does the system receive SBU/PII from State or local agency (-ies)?

No

Does the system receive SBU/PII from other sources?

No

Does the system receive SBU/PII from Taxpayer forms?

No

Does the system receive SBU/PII from Employee forms (e.g. the I-9)?

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

Yes

Does this system disseminate SBU/PII to other IRS Systems?

Yes

Identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name: ELITE - Enterprise Logistics Information Technology System (Tier 4 Application)
Current PCLIA: Yes
Approval Date: 12/4/2020
SA&A: No

System Name: Enterprise Application Integration Broker (EAIB) (Part of Enterprise System Domain (GSS-17))
Current PCLIA: Yes
Approval Date: 8/18/2021
SA&A: Yes
ATO/IATO Date: 8/28/2023

System Name: Business Entitlement Access Request System (BEARS)
Current PCLIA: Yes
Approval Date: 8/25/2021
SA&A: Yes
ATO/IATO Date: 4/20/2023

System Name: Taxpayer Advocate Management Information System (TAMIS)
Current PCLIA: Yes
Approval Date: 6/2/2020
SA&A: Yes
ATO/IATO Date: 3/14/2020

System Name: Integrated Data Retrieval System (IDRS)
Current PCLIA: Yes
Approval Date: 10/26/2021
SA&A: Yes
ATO/IATO Date: 11/1/2021

System Name: Compliance Data Warehouse (CDW)
Current PCLIA: Yes
Approval Date: 2/13/2023
SA&A: Yes
ATO/IATO Date: 5/10/2022

System Name: Automated Collection System (ACS)
Current PCLIA: Yes
Approval Date: 10/1/2021
SA&A: Yes
ATO/IATO Date: 12/1/2021

System Name: Automated Underreporter (AUR)
Current PCLIA: Yes
Approval Date: 6/7/2022
SA&A: Yes
ATO/IATO Date: 10/28/2021

System Name: Automated Trust Fund Recovery (ATFR)
Current PCLIA: Yes
Approval Date: 1/27/2020
SA&A: Yes
ATO/IATO Date: 6/25/2020

System Name: Security Auditing and Analysis System (SAAS)
Current PCLIA: Yes
Approval Date: 4/6/2020
SA&A: Yes
ATO/IATO Date: 4/29/2020

System Name: SPLUNK Enterprise (Streaming Data Monitoring Tool (SDMT))
Current PCLIA: Yes
Approval Date: 12/15/2021
SA&A: Yes
ATO/IATO Date: 3/7/2023

System Name: Affordable Care Act (ACA)
Current PCLIA: Yes
Approval Date: 5/7/2021
SA&A: Yes
ATO/IATO Date: 12/5/2022

Identify the authority.

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.

For what purpose?
AMS collects information from and disseminates information to IRS systems for the purposes of tax administration.

Does this system disseminate SBU/PII to other Federal agencies?

No

Does this system disseminate SBU/PII to State and local agencies?

No

Does this system disseminate SBU/PII to IRS or Treasury contractors?

No

Does this system disseminate SBU/PII to other Sources?

No

PRIVACY SENSITIVE TECHNOLOGY

Does this system use social media channels?

No

Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.?

No

Does the system use cloud computing?

No

Does this system/application interact with the public?

No

INDIVIDUAL NOTICE AND CONSENT

Was/is notice provided to the individual prior to collection of information?

Yes

How is notice provided? Was the individual notified about the authority to collect the information, whether disclosure is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects on the individual, if any, if they decide not to provide all or 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.

Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information?

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.

How does the system or business process ensure due process regarding information access, correction, and redress?

AMS receives data from other IRS upstream sources/systems. Those other sources/systems provide the Privacy Act Notice to individuals. Notice, consent and due process are provided via the IRS systems and their related tax forms instructions, and pursuant to 5 USC.

INFORMATION PROTECTION

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

The following people have access to the system with the specified rights:

IRS Employees

Users: Read Write

Managers: Read Write

System Administrators: No Access

Developers: Read Only

How is access to SBU/PII determined and by whom?

Business Entitlement Access Request System (BEARS) 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 BEARS. BEARS will then notify the manager of the request and the manager

will then approve the request via BEARS. The completed BEARS entitlement 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 the BEARS entitlement acknowledging his/her security responsibilities when using the system. The user signs security rules of behavior provided in BEARS. 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.

RECORDS RETENTION SCHEDULE

Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) approved a Records Control Schedule (RCS, IRS Document 12990) for the retention and destruction of official agency records stored in this system?

Yes

How long are the records required to be held under the corresponding GRS or RCS, and how are they disposed of? In your response, please provide the GRS or RCS chapter number, the specific item number, and records series title.

The Account Management Services application is comprised of four components: AMS Core; Correspondence Imaging System (CIS); Reasonable Cause Assistant (RCA); and Innocent Spouse (IS). 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 (AMS); RCS 19, Item 78 (Correspondence Imaging System (CIS)); RCS 28, Item 149 (Reasonable Cause Assistant (RCA)); RCS 29 Item 426 (Innocent Spouse (IS)) 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).

SA&A OR ECM-R

Has the system been through SA&A (Security Assessment and Authorization) or ECM-R (Enterprise Continuous Monitoring Reauthorization)?

Yes

What date was it completed?

6/13/2023

Describe 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); Internet Protocol (IP) Address; 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. The agent on the servers collects the data sending it to the audit logging system, Security Auditing and Analysis System (SAAS) and SPLUNK Enterprise.

PRIVACY TESTING

Does the system require a System Test Plan?

Yes

Is the test plan completed?

Yes

Where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)?

DocIt

Were all the Privacy Requirements successfully tested?

Yes

Are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved?

No

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 or SBU 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.

SBU DATA USE

Does this system use, or plan to use SBU Data in Testing?

No

NUMBER AND CATEGORY OF PII RECORDS

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

IRS Employees: Under 50,000

Contractors: Not Applicable

Members of the Public: More than 1,000,000

Other: No

CIVIL LIBERTIES

Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment?

No

Is the system information used to conduct 'data-mining' as defined in the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?

No

Will this system have the capability to identify, locate, and monitor individuals or groups of people?

No

Does computer matching occur?

No

ACCOUNTING OF DISCLOSURES

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