

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: June 19, 2014

PIA ID Number: **912**

1. What type of system is this? Legacy

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

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

Audit Information Management System-Reference, AIMS-R

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: _____

Number of Contractors: _____

Members of the Public: Over 1,000,000

4. Responsible Parties:

NA

5. General Business Purpose of System

Audit Information Management System Reference (AIMS-R) is a legacy Tier I system that processes information related to examinations of taxpayer accounts. Accounts can be established, updated, and closed online by authorized personnel using Integrated Data Retrieval System (IDRS) Real-time Command Codes. Discriminate Function (DIF) Orders and the Automatic Selection process also send accounts to AIMS, a subsystem of AIMS-R, to establish open cases in inventories. Due process is provided pursuant to 26 USC.

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: 08/23/2011

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 Yes
-

6c. State any changes that have occurred to the system since the last PIA

AIMS-R has a new system owner.

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

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 No

Other Source:

Other No

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	No
Social Security Number (SSN)	Yes	No	No
Tax Payer ID Number (TIN)	Yes	No	No
Address	Yes	Yes	No
Date of Birth	No	Yes	No

Additional Types of PII: No

No Other PII Records found.

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

The SSN is a unique identifier for each taxpayer that is required to file a tax return or is listed as a dependent on another's tax return. Tax return data for each taxpayer is accessed by the SSN.

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.)

IRC 6011, IRC 6109-1, 26 CFR Section 301.6109-1

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

There is no alternative solution.

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

There is no plan to eliminate the use of SSNs on this system.

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

Taxpayer Identification Number (SSN or EIN), taxpayer name, taxpayer address,

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.

Audit Trail Information – The Security and Communications System (SACS) maintains audit trail information for AIMS-R. This includes: user login/logoff; date/timestamp; IDRS codes used and transaction results.

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:

<u>System Name</u>	<u>Current PIA?</u>	<u>PIA Approval Date</u>	<u>SA & A?</u>	<u>Authorization Date</u>
ARR	Yes	04/03/2012	Yes	05/22/2012
BMF	Yes	03/18/2013	Yes	05/23/2013
CEAS	Yes	09/17/2012	Yes	12/06/2013
EARP	Yes	02/01/2012	No	12/06/2013
EPMF	Yes	11/10/2011	Yes	12/19/2011
ERCS	Yes	01/29/2014	Yes	04/10/2014
ERIS	Yes	11/10/2011	Yes	05/23/2012
GII (NA for ATO and PIA)	No	11/10/2011	No	05/23/2012
IDRS	Yes	07/12/2011	Yes	12/09/2011
IMF	Yes	05/02/2014	Yes	11/15/2012
LAND (non-app, NA for ATO and PIA)	No	05/02/2014	No	11/15/2012
LWIS	Yes	04/03/2012	Yes	06/07/2012
RCCMS	Yes	12/20/2012	Yes	02/22/2013
RICS	Yes	09/29/2011	Yes	02/01/2012
TRDB	Yes	11/28/2012	Yes	12/11/2012
CSTS (external)	No	11/28/2012	No	12/11/2012
AIS	Yes	04/21/2014	Yes	01/24/2014

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.

Each PII data item is required for the business purpose of the system. AIMS-R allows the designated end-users/employees of the SB/SE Operating Division, LB&I Operating Division, TE/GE Operating Division, W&I Operating Division and Appeals within the IRS who have been assigned a caseload related to their specific function

20. Did any of the PII provided to this system originate from any IRS issued forms? Yes

20a. If **Yes**, please provide the corresponding form(s) number and name of the form.

Form Number Form Name

20b. If **No**, how was consent granted?

Written consent _____

Website Opt In or Out option _____

Published System of Records Notice in the Federal Register _____

Other: _____

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:

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:	<u>Yes</u>	
Users		<u>Read Write</u>
Managers		<u>Read Only</u>
System Administrators		<u>Read Only</u>
Developers		<u>Read Only</u>
Contractors:	<u>No</u>	
Contractor Users		_____
Contractor System Administrators		_____
Contractor Developers		_____
Other:	<u>No</u>	_____

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?

Management determines which employees have access to AIMS-R and for what purposes. On Line (OL) Form 5081 documents at what levels users may view and use the data as a result of each employee who uses AIMS-R having a profile that determines this level of access.

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

The various programs and command codes within AIMS-R have built in validity checks to help ensure accuracy. For example, there are validity checks to ensure that an SSN/TIN entered into an on-line application contains all numeric data. A series of tests are performed on the data, such as a Unit Testing, Compatibility Testing, and Final Integration Testing to ensure the accuracy, timeliness and completeness of all IDRS data prior to its implementation during the annual Filing Season Start-up. If there is a discrepancy, an error record is generated. The error record is not included in the reports output.

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.

The procedures/requirements for eliminating the electronic TIF data at the end of the retention period are found in Document 12990, Records Control Schedule (RCS) 10 for Appeals, and RCS 23 for Tax Administration-Examination. Information ages off (is deleted from) the database at varying intervals. Current business practice is to retain data used for creating ARP and CF&S reports for a maximum of 365 days, after which data is erased from the cartridge. PCS is designed to ensure partnership adjustments are cascaded through to the related partners. Once all the partners are adjusted, the partnership information will drop off the system. For different data types, there are different retention periods. Retention schedules are documented in the Functional specification packages. After moving from the AIMS database, the data is moved to a cartridge and kept for 7 years. The IRS Records and Information Management (RIM) Office has requested a follow-up review of current records disposition procedures to ensure that business unit practice (as outlined in Functional specification packages) is in line with NARA-approved records control schedules and/or if instructions need to be updated.

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.
Security inherited from GSS.

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

AIMS-R uses Enterprise Disk Encryption (EDE) Software: The EDE project's purpose is to provide the IRS with an enterprise-wide solution for encryption of laptop hard drives and any computer that is managed or used outside of IRS controlled spaces, to prevent unauthorized access, in the case of loss or theft, to sensitive IRS information such as Personally Identifiable Information (PII). EDE is a hard disk encryption technology that specifically protects data at rest. The GSS-26 ERAP GSS employs Virtual Private Network technology to protect the confidentiality, integrity, and authenticity of remote data transmissions that contain sensitive information and also utilizes two factor authentication composed of something the user knows (password) and something the user has (grid card token) for authentication. For further details regarding the controls implemented for ERAP, see the GSS-26 Enterprise Remote Access GSS SSP.

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.

Ongoing Authorization (formerly eCM/eCM-r) testing is conducted each year. The SSP is reviewed annually and updated whenever there are significant changes to the system. As part of this ongoing authorization, the SSP is updated to ensure the security controls implemented for the system are accurately reflected, all applicable NIST SP 800-53 controls are addressed, and the document is compliant with NIST SP 800-18. The IS Contingency Plan (ISCP), Security Control Assessment (SCA) Plan, SCA Results Matrix and Security Assessment Report (SAR) are developed in accordance with NIST methodology.

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*)? Yes

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.

IRS 22.054	Subsidiary Accounting Files
IRS 22.060	Automated Non-Master File
IRS 22.061	Information Return Master File
IRS 22.062	Electronic Filing Records
IRS 24.030	Customer Account Data Engine Individual Master Fil
IRS 24.046	Customer Account Data Engine Business Master File,
IRS 26.019	Taxpayer Delinquent Accounts Files
IRS 42.001	Examination Administrative File
IRS 42.008	Audit Information Management System
IRS 34.037	IRS Audit Trail and Security Records System

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)	<u>No</u>
Provided viable alternatives to the use of PII within the system	<u>No</u>
New privacy measures have been considered/implemented	<u>No</u>
Other:	<u>No</u>

32a. If **Yes** to any of the above, please describe:

NA