AIMS Computer Information System (A–CIS) – Privacy Impact Assessment

PIA Approval Date – Jul. 24, 2009

System Overview

The Audit Information Management System (AIMS) – Computer Information System (A–CIS) was developed as a monitoring and reporting tool used to perform detailed analysis of tax cases within examination; detailed analysis of case inventory levels; to monitor the examination process; and to effectively plan for ongoing examination operations. The application contains data retrieved from the Closed AIMS, Open AIMS, and Non–Examined AIMS databases (DB) retrieved from the Audit Information Management System – Reference (AIMS–R) application; and Summary Examination Time Transmission System (SETTS) data retrieved from the Examination Returns Control System (ERCS). A–CIS allows its users to generate reports on case information by selecting options from drop down menus in the application's front–end user interface. By modifying the criteria used to select the case information, A–CIS users can create an unlimited number of different reports tailored to their individual needs.

Systems of Records Notice (SORN):

- IRS 42.008--Audit Information Management System
- IRS 34.037--IRS Audit Trail and Security Records System

Data in the System

1. Describe the information (data elements and fields) available in the system in the following categories:

A. Taxpayer:
- Taxpayer identification number (TIN)
- Name
- Claim amount
- Tax owed/Tax refunded amount
- Amount of tax credit adjustment
- Adjustment amount
- A two digit code that identifies the tax form number
- Zip code
- State
- Address
- Total positive income
- Some state tax return information
- State housing credit allocation information

B. Employee:
- AIMS Assignee Code (AAC) (A twelve–digit code used for the management structure so that returns and time applied to returns can be applied to the correct location (Business Operating Division, Area Director, Field Operations Director (LMSB), Territory Manager, Group number) for management information reports.)

C. Audit:
- Auditing occurs at the A–CIS system level and the GSS level. The A–CIS logs capture C2 audited events. The A–CIS audit logs (trace files) are transferred to the Quest repository by Data Management Group 8 Security and stored for no less than 7 years.

(Why so long when the actual records are only kept five years (see question 13). Additionally, audit logs of users who access the A–CIS application are captured by the A–CIS operating system's security logs which are maintained by the Modernization & Information Technology Services (MITS)–30 General Support Services (GSS). These logs are reviewed per Domain Level GSS common controls. Does this system have Negative Tin checking?

- For the Enterprise Application Support Servers, Data Management Group 8 is responsible for collecting the audit logs generated by the servers. The Mission Assurance office (Mission Assurance was dissolved 3 years ago. This needs to be rewritten/changed. ensures the Enterprise Application Support Servers application audit tools create, maintain, and protect a trail of actions produced by users and administrators that trace security–relevant events to an individual, ensuring accountability. These tools are part of the operating system and log auditing events for telecommunication and other components. Data Management Group 8 auditing captures user workstation and log on/off activities. It also logs system administrator and security administrator activities. The audit logs capture critical event information (type of event, source of event, time and date of event, user accountable for event) that is useful for identifying system intrusion detection and system forensics should an attack occur. Logs are regularly reviewed. The logs are stored in a flat file in the application directory of a Unix server.

D. Other:
   - State housing credit agency EIN, name and address
   - Building Identification Number (BIN) used to identify low–income buildings receiving IRC §42 credit allocations
   - State Identification Number
   - Preparer's TIN

2. Describe/identify which data elements are obtained from files, databases, individuals, or any other sources.

A. IRS:
   - AIMS:
     - TIN
     - Taxpayer name
     - Claim amount
     - Tax owed/Tax refunded amount
     - Adjustment Amount
     - Zip code
     - State
     - Total positive income
     - AIMS Assignee Code
   - ERCS: (SETTS data)
     - Employee ID
     - AIMS Assignee Code

B. State and Local Agencies: The State Reverse File Match Initiative (SRFMI) and Low–Income Housing Credit (LIHC) databases will receive information from state agencies.
   - Taxpayer Name, Address and EIN

- Some state tax return information list what state tax return info will be included, not "some"
- IRC §42 credit allocation information, including the Building Identification Number
- State housing credit agency EIN, name and address
- State Identification Number
- Preparer's TIN

3. Is each data item required for the business purpose of the system? Explain.
Yes, A–CIS provides MIS data and inventory information to IRS employees to analyze examination inventory levels and examination results. In the future A–CIS will provide possible workload selection data and housing credit information to IRS employees.

4. How will each data item be verified for accuracy, timeliness, and completeness?
The data is not verified for accuracy, timeliness, or completeness by A–CIS. The data is validated on the AIMS system from which it is extracted. If an error exists in the data received from the AIMS or SETTS data, the A–CIS developer sends an email to the AIMS and SETTS personnel for research and resolution. Upon resolution, the A–CIS developer then notifies the end user. Discretionary checks of the data are performed by the A–CIS Database Administrator (DBA) and personnel from the Examination Management Information section. For SRFMI data, validation checks will be performed prior to the data being copied to the A–CIS server. For LIHC data, validation checks will be performed prior to the data being copied to the A–CIS server.

5. Is there another source for the data? Explain how that source is or is not used.
No. There is no other source for this data than what has been stated previously in this document.

6. Generally, how will data be retrieved by the user?
End users download the MS Access database(s) that they have permissions to browse (I suggest another word other than "browse" what about "review" or they work off the server directly. Users either use an Access front–end or they go in through Excel or Access directly. Retrieval procedures consist of the standard query methods used in database applications.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?
Yes. Data is retrievable using any data elements in the system, to include personal identifiers such as TIN and taxpayer name.

<u>Access to the Data</u>
8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?

Role: System Administrator
Permission: Read, Write, Delete, Add User

Role: End–user /Analyst
Permission: Online Database: Read Database Downloaded to Workstation: Read, Modify, Print, Save

Note: Contractors do not have access to the application.

9. How is access to the data by a user determined and by whom?
A–CIS relies on the GSS common controls associated with the IRS Enterprise Active Directory domain structure to uniquely identify and verify the identity of each user. An OL5081 is required of IRS users requesting access to A–CIS and must be signed by an immediate manager and Small Business/Self–Employed (SB/SE) Exam managers. Once forms are approved they are submitted to the MITS system administrator and application administrator, who adds the new user's account into the system. The OL5081 process ensures that the user identifier is issued to the intended party and that user identifiers are archived. A–CIS also relies on GSS common controls to enforce the disabling of user accounts that have been inactive for 45 and 90 days. According to the GSS common controls, User accounts that are inactive for a period of 45 days are disabled. User accounts that are inactive for a period of 90 days are deemed expired accounts and are removed from the application.

For access to A–CIS, users must first successfully authenticate to their respective campus domain GSS infrastructure utilizing their IRS account provided trough the Online 5081 process. Once successfully authenticated to the campus domain, A–CIS users are transparently given the proper permissions, through domain group policy, to access the A–CIS application databases to run queries and generate reports. Authorized A–CIS users are uniquely identified and placed in domain groups by a MITS System Administrator via the Online 5081 process. Before the MITS System Administrator receives the list of users via the Online 5081 process, the form 5081 is approved at various levels in SB/SE and the BOD of the employee requesting access to the data. To access the A–CIS backend server SQL database, application developers must submit and have an approved Online 5081. MITS personnel are responsible for adding the approved users to the proper A–CIS SQL SA groups. The new databases will be similar. The SRFMI database might be working with a contractor in late FY2009. If so, they will follow all established policies and procedures.

10. Do other IRS systems provide, receive, or share data in the system? If YES, list the system(s) and describe which data is shared.
There are no direct interconnections from A–CIS to other applications. Audit Information Management System (AIMS) and Summary Examination Time Transmission System (SETTS) data is copied to the A–CIS windows server via file system transfer from a desktop computer in National Office by personnel on the AIMS staff. All AIMS data is retrieved from the Audit Information Management System Reference (AIMSR) application. The specific data type copied from Examination Returns Control System (ERCS) is SETTS. These data files received by the A–CIS application are the support for AAR (AIMS Related Report) and ARP (AIMS Related Processing). State Reverse File Match Initiative (SRFMI) and Low–Income Housing Credit (LIHC) data will be copied to the A–CIS windows server from a development server.

11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?

Audit Information Management System Reference (AIMSR) (AIMS is a component of AIMSR)
- Certification & Accreditation (C&A) – May 1, 2009
- Privacy Impact Assessment (PIA) – February 11, 2009

Examination Returns Control System (ERCS) (SETTS is a component of ERCS)
- Certification & Accreditation (C&A) – May 29, 2008
- Privacy Impact Assessment (PIA) – March 3, 2008

12. Will other agencies provide, receive, or share data in any form with this system?
A–CIS must provide information to the U.S. Treasury Inspector General for Tax Administration (TIGTA) if requested. This information, however, is not provided directly by A–CIS, but rather by a

user or system administrator who would query for the information and then provide it directly to TIGTA. Otherwise, A–CIS does not have any interconnections outside the IRS boundary.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?
Records are destroyed in accordance with IRM 1.15.23 Examination #6 (Records Control Schedule for Tax Administration, Administrative Records). This portion of the IRM states that the following types of records will be destroyed after five years. Monthly, Quarterly, Annual, and Other Periodic Management Information Reports. Includes computer generated reports produced from the Master File and other Management Information Systems of the Service to measure field accomplishments in returns and staff time, additional taxes and penalties proposed, and effected and related material. (Job No. N1–58–88–2, Item 6).

14. Will this system use technology in a new way?
No. This system does not use technology in a new way.

15. Will this system be used to identify or locate individuals or groups? If so, describe the business purpose for this capability.
Yes. A–CIS can be used to identify an entity (an individual or a business). A–CIS is sometimes used for inventory information (open or closed) so this information is needed. State Reverse File Match Initiative (SRFMI) data will be used for workload selection so this information is needed.

Low–Income Housing Credit (LIHC) data provides information regarding the allocation of tax credits by state housing credit agencies and the taxpayers owning qualified low–income properties. This information is used for program administration and workload selection so this information is needed.

16. Will this system provide the capability to monitor individuals or groups? If yes, describe the business purpose for this capability and the controls established to prevent unauthorized monitoring.
No. A–CIS will not be used to monitor individuals or groups.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?
No. A–CIS will not be used to allow IRS to treat taxpayers, employees, or others, differently. All users will be required to follow National Office documents, including the IRM, directives, and memoranda.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?
A–CIS does not make any negative determinations.

19. If the system is web–based, does it use persistent cookies or other tracking devices to identify web visitors?
No. This system is not web–based and therefore uses no cookies of any type.

View other PIAs on IRS.gov