Automated Insolvency System (AIS) – Privacy Impact Assessment

PIA Approval Date – July 30, 2010

System Overview:

Automated Insolvency System (AIS) the IRS's primary tool for tracking legal requirements for dealing with taxpayers under bankruptcy protection as well as ensuring that the government's interest is protected when these taxpayers have tax obligations. AIS is a comprehensive control and processing support application for processing bankruptcy and other insolvency work. It provides case inventory, status control, proofs of claim, and exchange of information with the United States Bankruptcy Court's Case Management/Electronic Case Filing (CM/ECF) system. One of the primary functions of the application is to prepare and file proofs of claim with the U.S. Bankruptcy Court.

Systems of Records Notice (SORN):

- IRS 26.009--Lien Files
- IRS 26.019--Taxpayer Delinquent Account Files
- 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 Data includes:
   - TIN or cross–reference SSN (if the cross–reference social security number (SSN) was the primary TIN in Integrated Data Retrieval System (IDRS)) for claim records, compliance checks or credit records
   - Name
   - Address
   - Tax Amount
   - Interest Amount
   - Penalty Amount
   - System ID of the user who is running an Automated Proof of Claim (APOC)
   - Case ID (unique) assigned to the record

B. Employee – AIS contains the name, login name, badge number, email address, standard employee identification (SEID), and work telephone number of the employee assigned to the case.

C. Audit Trail Information – The system collects the following audit trail data items:
   - employee log–in information
   - any actions taken by the employee
   - date of the activity

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

A. IRS – Lien information comes from Automated Lien System (ALS). ALS provides:
   - Name
   - Residence

- Author
- Tax Period
- TIN

Taxpayer information comes from Auditing Information Management System (AIMS). AIMS provides:

- Name
- TIN
- Special Project Code

Taxpayer information comes from IDRS/Masterfile. IDRS/Masterfile provides:

- Taxpayer Name
- Name Control
- Secondary TIN
- Primary SSN
- TSIGN
- Cross reference (xRef) TIN
- TIN Name Control
- Other taxpayer module information

B. Taxpayer – Taxpayer information comes from taxpayer filed forms and correspondence.

C. Employee – The employee supplies the name of the employee assigned to the case.

D. Other Federal Agencies – Taxpayer information is collected through the U.S. Bankruptcy Courts. This information includes:

- SSN
- TIN
- Address
- Petition Date
- Trustee Name,
- Trustee Address
- Trustee Phone
- Attorney Name
- Attorney Address
- Attorney Phone
- Amount

E. Other Third Party Sources – US Bankruptcy courts, attorneys and trustees provide data.

3. Is each data item required for the business purpose of the system? Explain.
Yes. All data items are necessary to process and control insolvency cases.

4. How will each data item be verified for accuracy, timeliness, and completeness?
Data will be visually inspected and corrected manually when errors are encountered. Validity checks for timeliness and completeness are completed on the data prior to and while it is loaded into AIS. The input load program checks to verify that numeric and alphanumeric fields are populated by numeric and alphanumeric entries respectively. These entries are verified for correctness both before and during processing in AIS. AIS employs rules to check the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) to verify that inputs match

specified definitions for format and content and pre–screens inputs passed to interpreters to prevent the content from being unintentionally interpreted as commands. No processes are executed when invalid responses are entered.

5. Is there another source for the data? Explain how that source is or is not used.
No. There are no other sources of data.

6. Generally, how will data be retrieved by the user?
The data is generally retrieved via a query or report using the case number or taxpayer identification number (TIN).

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?
Yes, the data is retrievable by Taxpayer Identity Number (TIN).

Access to the Data

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?
Users, managers, systems administrators, developers, and program analysts will have access to the AIS system.

Role: User
Permission: Users shall have access to AIS components based on each individual user's security profile; One through Four. Level One allows full access to taxpayer case–related screens, full query access and some add/update access to support tables, permission to generate or print most reports, and all forms and letters. Level Two allows full access to all taxpayer related screens, query access to support tables, and permission to generate or print some reports, forms and letters. Level Three allows full access to taxpayer case–related screens, no access to support table menus, and no access to bulk generation/print options. Level Four is restricted to read/query access to taxpayer case–related information.

Role: Manager
Permission: Managers have Level One access to all reports and audit tracking information and additional manager permission with the added capability of User Administration privileges.

Role: Analyst
Permission: Analysts have Level One, Manager access permissions and the capability to control support data.

Role: User Admin
Permission: User Administrators have the ability create accounts, change passwords, and delete users.

Role: IIP User
Permission: The IIP user has access to the IIP subsystem which requires a separate log–in directly into database server using a Sun Solaris account. The user uses telnets (Info Connect) to open a session on the database server to gain access to the IIP Menu interface in order to execute C/C+ code. The menu interface provides SACS (Security and Communication System) authentication to IDRS via the user's logon credentials. The IIP process, initiated by the IIP user, will then import data from IDRS and performs TIN/SSN validation, make collection

determinations based on the information from IDRS, and freeze IRS systems from sending notices when necessary.

Role: ADS User
Permission: The ADS user has access to the ADS subsystem which requires a separate log–in directly into database server using a Sun Solaris account. The user uses telnets (Info Connect) to open a session on the database server to gain access to the ADS Menu interface in order to execute C/C+ code. The menu interface provides SACS (Security and Communication System) authentication to IDRS via the user's logon credentials. The ADS process, initiated by the ADS user, accesses IDRS information and takes the appropriate actions needed to discharge and close cases.

Role: Developer
Permission: Developers are responsible for the ongoing maintenance of AIS application source code and manage the data exchange batch process for the application. Developers do not function as end users within AIS.

Role: APOC Operator
Permission: The APOC operator role allows the user to see and update the internal APOC database tables. Internal APOC tables are calculation areas that AIS cannot see until APOC transfers the data to the AIS database tables. Usually this transfer is an automated procedure, but sometimes issues arise that require human intervention before the data can be given over to AIS. This human intervention is the primary purpose of the APOC web Interface. The Batch program also makes use of the APOC operator role as well as UNIX level security. To get to the APOC Batch program, one must first have a UNIX account on the database server; this is a very small population. To ensure APOC users are the only people that can start the Batch program, a validation is performed to determine if the end user has access to the role APOC operator.

Role: EPOC User (Local /Global DS Group)
Permission: EPOC Users are located in Philadelphia, PA. The EPOC User sends proof of claim documents (B10/6338 or 6338A) to U.S. Bankruptcy Courts CM/ECF. Access to CM/ECF is coordinated locally with the U.S. Bankruptcy courts. Users are required to submit login applications to each U.S. Bankruptcy court for CM/ECF privileges and are provided website documentation and training by the U.S. Bankruptcy courts. The EPOC User selects an EPOC icon on their desktop and the application accesses the appropriate directory on the EPOC Server where all queued proof of claim documents are located to be sent to a specific U.S. Bankruptcy court. The application then logs on to the U.S. Bankruptcy court website and selects a case for processing. The EPOC application sends case related data and a claim document in .pdf format. The CM/ECF website receives the information and sends an acknowledgement back to the EPOC Server and EPOC writes an acknowledgment to be loaded into AIS.

Role: DBAs/SAs
Permission: DBAs do not have access to the standard functionality within AIS. DBAs only have access to those functions that relate to the maintenance of the application and the underlying hosting environment. DBAs do not have user accounts in AIS.

Note: All users of the application are IRS employees and are located within the IRS firewall. Contractors do not have access to the AIS application.

9. How is access to the data by a user determined and by whom?
Access to the data is determined by the manager based on a user's position and need–to–know. The manager will request a user be added. In order to gain access, an approved Online Form 5081 and Information System User Registration/Change Request is required. A user's access to the data terminates when it is no longer required. Criteria, procedures, controls, and responsibilities regarding access are documented in the Information Systems Security Rules on Form 5081.

Note: There are no contractors acting as users of the system.

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.

- Integrated Data Retrieval System (IDRS) – Information retrieved from IDRS/Masterfile by IIP to AIS. This retrieval is completed daily and is manually initiated by AIS users. Masterfile information is received automatically on a weekly and quarterly basis.
- Automated Discharge System (ADS) – Information retrieved from IDRS/Masterfile by ADS is provided to AIS. This retrieval is completed daily and is manually initiated by AIS users. Masterfile information is received automatically on a weekly and quarterly basis.
- Insolvency Interface Program (IIP) – Taxpayer information extracted from AIS is utilized by the IIP and ADS to update the IDRS.
- Automated Lien System (ALS) – Lien information is sent to and returned automatically from ALS daily.
- Insolvency Notification System (INS) – receives data once per week via EFTU from AIMS which contains taxpayers under audit. A weekly match of audit and bankruptcy information is also run and AIS may be updated with new AIMS information.

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

Integrated Data Retrieval System (IDRS)

- Certification & Accreditation (C&A) – May 10, 2009
- Privacy Impact Assessment Date (PIA) – November 6, 2008

Automated Lien System (ALS) Entity

- Certification & Accreditation (C&A) – May 24, 2008
- Privacy Impact Assessment Date (PIA) – December 20, 2007

Auditing Information Management System (AIMS)

- Certification & Accreditation (C&A) – May 1, 2009
- Privacy Impact Assessment Date (PIA) – April 8, 2009

12. Will other agencies provide, receive, or share data in any form with this system?
Yes. Taxpayer information is collected through the Bankruptcy Courts. The Bankruptcy Courts transmit the information to the U.S. Bankruptcy Courts Noticing Center where AIS retrieves the data. Data is sent electronically to U.S. Bankruptcy Courts as required by individual Courts.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?
AIS data is currently approved for destruction six years after case is closed (Job No. N1–58–97–13, item 35, and published under IRM 1.15.35, item 35). However, new requirements under the Bankruptcy Abuse Prevention and Consumer Protection Act (BAPCPA) require that data be maintained for eight years after case is closed. To that end, a request for an extension to the currently approved retention is currently being drafted with the assistance of the IRS Records and Information Management (RIM) Program Office. When approved by the National Archives and Records Administration (NARA), updated disposition instructions for AIS data will be re–published under IRM 1.15.35, item 35.

14. Will this system use technology in a new way?
No. AIS 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, the system is used to identify or locate individuals or businesses that are under bankruptcy protection but still have tax obligation. AIS is used to prepare and file proofs of claim with the U.S. Bankruptcy court. AIS provides case inventory, status control, proofs of claim, and exchange of information with the United States Bankruptcy Court's Case Management/Electronic Case Filing (CM/ECF) system.

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.
Yes, the system provides the capability to monitor individuals. One of the business purposes of AIS is to monitor the status of the insolvency. All IRS employees must conform with Unauthorized Access (UNAX) regulations for accessing taxpayer information. There is annual mandatory UNAX training for all IRS employees. IRS employees must sign a form indicating they have taken the training.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?
No. AIS does not have the ability to allow IRS to treat taxpayers, employees, or others differently.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?
AIS does not impact due process rights of taxpayers/employees. AIS is a collection and tracking system that is used to process and control bankruptcy and other insolvency cases.

19. If the system is web–based, does it use persistent cookies or other tracking devices to identify web visitors?
The application is web–based and does use session–only cookies; however it does not use persistent cookies or other tracking devices to identify web visitors. This application is an internal IRS web–based application; it is not outward–facing.

View other PIAs on IRS.gov