

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: 04/15/2014 PIA ID Number: 824

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):

Automated Insolvency System - Mod, AIS

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: Under 50,000

Number of Contractors: Not Applicable

Members of the Public: Not Applicable

4. Responsible Parties:

NA

5. General Business Purpose of System

Automated Insolvency System (AIS) is a web-enabled database application utilizing Oracle 11g application and database servers to include Oracle Forms and Reports and the Weblogic server version 10.3.4 that assist the Small Business/Self-Employed (SB/SE) division in managing the life cycle of a taxpayer bankruptcy case process as it relates to the IRS and resides on the GSS-24. The AIS application contains personally identifiable information (PII) data (e.g., taxpayer identification numbers (TIN) and social security numbers (SSNs)), which are processed, stored, and transmitted through the application and are used in the processing of bankruptcy and other insolvency proceedings. AIS is 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. The AIS application 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. The AIS application is comprised of multiple processes that perform specialized functions and/or interface with internal and external systems. The processes that make up AIS are the Electronic Notice System (ENS), Insolvency Notification System (INS), Litigation Account Management System (LAMS), Litigation Transcript System (LTS), and Case Assignment Guide (CAG). The descriptions of the functionalities are as followed:

- *AIS interfaces with Automated Liens System – Entity Case Management System (ALS-Entity) to retrieve a list of new case taxpayer identification number (TINS) for lien research and provides lien facsimiles for when TINS are found within ALS-Entity. Lien information is transmitted to and from AIS via Electronic File Transfer Utility (EFTU).
- *ENS processes bankruptcy notices, in the form of the Electronic Data Information (EDI), from the Defense Logistics Agency (DLA) system via the EFTU. The DLA server uploads the bankruptcy notices into the common drop box servers, located at ECC-MEM and ECC-MTB. The EFTU process performs daily transfer of these notices from the common drop box servers to AIS. Once translated, the EDI data is distributed to the correct AIS directories for processing.
- *INS receives data once per week via EFTU from the Audit Information Management System – Reference (AIMS-R) which contains taxpayers under audit. A weekly match of audit and bankruptcy information is also run and AIS may be updated with new AIMS-R information.
- *LAMS receives data from both the Individual Master File (IMF) and the Business Master File (BMF) via EFTU on a quarterly basis. The LAMS application also provides information on unreversed 520 transaction codes.

- *LTS receives data from both the IMF and the BMF and provides transcripts of information. This data is imported into AIS on a weekly scheduled process via EFTU.
- *CAG grades new bankruptcy cases based upon preset criteria and assigns the new cases to users based upon grade. The sections below denotes the components that make up the AIS application: Automated Discharge System (ADS); Automated Proof of Claim (APOC); Insolvency Interface Program (IIP); and Electronic Proof of Claim (EPOC). Automated Discharge System (ADS) - ADS accesses the Integrated Data Retrieval System (IDRS) information and takes the appropriate actions needed to discharge and close cases. Automated Proof of Claim (APOC) - APOC accesses IDRS through user initiated commands via Unix menus. APOC is used to prepare proof of claim data. Insolvency Interface Program (IIP) - IIP imports data from IDRS and performs TIN/SSN validation, makes collection determinations based on the information from IDRS, and freezes IRS systems from sending notices when necessary. Electronic Proof of Claim (EPOC) - EPOC is a sub-system of AIS that is utilized to interface with the U.S. Bankruptcy Courts CM/ECF system for U.S. Bankruptcy courts that require electronic claim filing. AIS users initiate proof of claim batch processes as needed (daily). Proofs of claims are held in a queue until they are transmitted to a U.S. Bankruptcy court's CM/ECF website through the EPOC sub-system. The EPOC sub-system uploads case related data and proof of claims in Adobe .pdf format via the US Bankruptcy Courts' web site. Acknowledgements are received from the CM/ECF. 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: 07/23/2010

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

Creating a new PIA entry for AIS in the Privacy Assessment Management System (PIAMS).

7. If this system has an Exhibit 53 or Exhibit 300 please provide the Unique Project Identifier (UPI) number (XXX-XX-XX-XX-XX-XXXX-XX). Otherwise, enter the word 'none' or 'NA'. 015-45-01-14-02-2289-00

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

8a. If No, what types of information does the system collect, display, store, maintain or disseminate?

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	<u>Yes</u>
Employees/Personnel/HR Systems	<u>No</u>
Other	<u>Yes</u>

Other Source:

US Bankruptcy Courts

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

Additional Types of PII: No

PII Name On Public? On Employee?

No No

10a. Briefly describe the PII available in the system referred to in question 10 above.

N/A

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.)

Treasury/IRS 26.009 Lien Files Treasury/IRS 26.019 Taxpayer Delinquent Account Files Treasury/IRS 34.037 IRS Audit Trail and Security Records System

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

No alternatives have been identified.

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

No mitigation strategy has been identified at this time.

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.

Application Level Implementation (Portion of Main Control Objective): FROM SSP v2.7 – Control AU-2 Due to the configuration of the AIS application, only a limited number of auditable events are logged at the application level. The application-level auditing that is currently taking place: - Log onto System - Log off of System - Change of Password - All system administrator (SA) actions, while logged on as an SA - Sub-set of security administrator actions, while logged on in the security administrator role - Clearing of the audit log file - Startup and shut down of Audit Functions - Application critical record changes - All system and data interactions concerning taxpayer data All other auditable events are logged by the System Administrators of the GSS-24. The Audit Trails produced by AIS maintain a record of system activity and are created, maintained, and protected from modification and unauthorized access.

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:

No System Records found.

b. Other federal agency or agencies: Yes

If Yes, please list the agency (or agencies) below:

US Bankruptcy Courts

c. State and local agency or agencies: No

If Yes, please list the agency (or agencies) below:

d. Third party sources: No

If yes, the third party sources that were used are:

e. Taxpayers (such as the 1040): Yes

f. Employees (such as the I-9): Yes

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.

AIS contains Personally Identifiable Information (PII) (e.g., Taxpayer Identification Numbers (TINs) and Social Security Numbers (SSNs)), which is processed, stored, and transmitted through the application and is used in the processing of bankruptcy and other insolvency proceedings.

D. PII USAGE

Authority: OMB M 03-22 & PVR #16, Acceptable Use

14. What is the specific use(s) of the PII?

To conduct Tax Administration	<u>Yes</u>
To provide Taxpayer Services	<u>Yes</u>
To collect demographic Data	<u>Yes</u>
For employee purposes	<u>Yes</u>

Other:

No

If other, what is the use?

E. INFORMATION DISSEMINATION

Authority: OMB M 03-22 & PVR #14- Privacy Notice and #19- Authorizations

15. Will the information be shared outside the IRS? (for purposes such as computer matching, statistical purposes, etc.) Yes

15a. If yes, with whom will the information be shared? The specific parties are listed below:

	Yes/No	Who?	ISA OR MOU**?
Other federal agency (-ies)	Yes	US Bankruptcy Courts through Defense Logistics Agency (DLA)	Yes
State and local agency (-ies)	No		
Third party sources	No		
Other:	No		

** Inter-agency agreement (ISA) or Memorandum of Understanding (MOU)

16. Does this system host a website for purposes of interacting with the public? Yes

17. Does the website use any means to track visitors' activity on the Internet? No

If yes, please indicate means:

	YES/NO	AUTHORITY
Persistent Cookies	<u>No</u>	<u></u>
Web Beacons	<u>No</u>	<u></u>
Session Cookies	<u>No</u>	<u></u>
Other:	<u>No</u>	<u></u> <i>If other, specify:</i>

F. INDIVIDUAL CONSENT

Authority: OMB M 03-22 & PVR #15- Consent and #18- Individual Rights

18. Do individuals have the opportunity to decline to provide information or to consent to particular uses of the information? No

18a. If Yes, how is their permission granted?

19. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action? Not Applicable

19a. If Yes, how does the system ensure "due process"?

20. Did any of the PII provided to this system originate from any IRS issued forms? No

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

No forms found.

20b. If No, how was consent granted?

Written consent	<u>No</u>
Website Opt In or Out option	<u>No</u>
Published System of Records Notice in the Federal Register	<u>No</u>
Other: <u>US Bankruptcy Courts through Defense Logistics Agency (DLA)</u>	<u>Yes</u>

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: IRS Owned and Operated

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 Write</u>
System Administrators		<u>Read Write</u>
Developers		<u>Read Only</u>
Contractors:	<u>No</u>	
Contractor Users		<u></u>
Contractor System Administrators		<u></u>
Contractor Developers		<u></u>
Other: <u>Revenue Officers and any other IRS employees who would need information.</u>	<u>Yes</u>	<u>Read Only</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? No

23. How is access to the PII 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 On-Line 5081 Form.

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

Internal cross reference with other IT systems and visual inspections.

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.

AIS data is approved for destruction eight years after case is closed (Job No. N1-58-10-21, approved 9/13/2010). This represents an update to the six-year disposition earlier approved under Job No. Job No. N1-58-97-13. New requirements under the Bankruptcy Abuse Prevention and Consumer Protection Act (BAPCPA) require that data be maintained for eight years after case is closed. When next published, updated disposition instructions for AIS data will be included under IRM 1.15.35, item 35 (look for transition of this IRM to Records Control Schedule Document 12990 under RCS 35 soon). Automated Insolvency System (AIS) AIS contains and processes information on bankruptcy court cases. The database contains information related to bankruptcy and insolvency cases, i.e., basic case and taxpayer account information, case histories, proof of claim data, and payment information (Delete 8 years after case is closed). Program Office Supported by the system: Collection A. Input Records: These records include electronic transfer of data from Masterfile/IDRS, court notices (electronic or hard copy), plus status information entered manually by Collection employees (Delete/destroy when 1 year old or when no longer needed for

administrative; legal, audit or other operational purposes whichever is sooner). B. Output Records: Transaction code inputs and voucher payments to IDRS, proof of claims filed with court, letters to taxpayers and attorneys, plus system backups, management information reports, program-related reports, ad hoc queries, Audit Trail, or equivalent documentation in electronic or hard copy formats (Delete/destroy when 1 year old or when no longer needed for administrative, legal, audit or other operational purposes whichever is sooner).

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.

Periodic background check. Security inherited from GSS.

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

Security inherited from GSS. AIS resides on Sun servers at TCC.

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.

In accordance with IRM 10.8.1.3.1 (3) and NIST SP 800-30, risk assessments are reviewed on an annual basis and updated on a periodic basis (at a minimum of every three years), commensurate with the sensitivity and criticality of the data processed. Risks are reassessed when there is a major change to the application or the GSS(s) on which the application resides, or due to other conditions that may have an impact on the application's security posture. Risks associated with the infrastructure controls were identified in the GSS risk assessment(s) that were performed for the GSS-24 on which the application resides.

29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 - IT Security, Live Data Protection Policy? Yes

29a. Has approval been received from the Office of Privacy Compliance to use Live Data in testing (if appropriate)? No

29b. If you have received permission from the Office of Privacy Compliance to use Live Data, when was the approval granted? 10/01/2011

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.

SORNS Number

SORNS Name

Treasury/IRS 26.009 Lien Files

Treasury/IRS 26.019 Taxpayer Delinquent Account Files

Treasury/IRS 34.037 IRS Audit Trail and Security Records System

Comments

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:

Not Applicable

[View other PIAs on IRS.gov](#)