Date of Approval: **January 07, 2022**

PIA ID Number: **6638**

SYSTEM DESCRIPTION

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

Insolvency Interface Program, IIP

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?

Insolvency Interface Program, IIP, PCLIA #3897

What is the approval date of the most recent PCLIA?

2/18/2019

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.

IIP reports to the Applications Development (AD) Internal Management Domain Change Control Board/Governance Board meeting and elevated items to the Sustaining Operations Executive Steering Committee.

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?

No

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 Insolvency Interface Program (IIP) automates the transfer of data between the Automated Insolvency System (AIS), an Oracle database, and Integrated Data Retrieval System (IDRS). IIP goes beyond the mere transfer of data - it includes processing and decision-making based upon the value of the data it is processing. Additionally, IIP may alter or abort a processing sequence in one system based upon the value, existence, or non-existence of data in the other system. IIP also facilitates bankruptcy research and IDRS terminal input. It is an effort to automate time-consuming tasks normally performed by clerical and bankruptcy specialists.

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

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

IIP requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns.

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 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. IIP requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer at this time.

Employer Identification Number

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
Standard Employee Identifier (SEID)
Tax Account Information

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:

Agency Sensitive Information Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission.

Official Use Only (OUO) or Limited Official Use (LOU) Information designated as OUO or LOU is information that: is exempt under one of the statutory Freedom of Information Act exemptions; is prohibited by other laws or regulations; would significantly impede the agency in carrying out a responsibility or function; or would constitute an unwarranted invasion of privacy.

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?

No

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

Has the authority been verified with the system owner?

Yes

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.

Relevant SBU/PII is used to conduct bankruptcy processing. Specifically: Name is used to identify taxpayers who have filed for bankruptcy. Mailing address is used to identify taxpayers who have filed for bankruptcy. Standard Employee Identifier (SEID) is used to identify the IRS employee who is assigned the case. Tax account information is used to complete bankruptcy processing for the taxpayer.

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

The data that IIP receives is from Internal Revenue Service (IRS) systems (IDRS & Computer Files On Line (CFOL)) which are deemed reliable, and the data is validated for accuracy by the system sending the data as described in that system's Privacy and Civil Liberties Impact Assessment. Any determinations made are validated during IIP processing and the taxpayer has appeal rights for any determinations made from the data.

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.

IRS 26.019 Taxpayer Delinquent Account Files

IRS 34.037 Audit Trail and Security Records

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

Official Use Only

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

System Name: Computer Files On Line (CFOL)
Current PCLIA: No
SA&A: No

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: Automated Insolvency System (AIS)
Current PCLIA: Yes
Approval Date: 2/18/2020
SA&A: Yes
ATO/IATO Date: 7/15/2019

Identify the authority.

The authority for processing taxpayer information is title 5 U.S.C. 301 and title 26 U.S.C. 7801.

For what purpose?

The purpose for sharing taxpayer information with AIS is to facilitate bankruptcy processing.

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 IRS notifies all individuals who file tax returns of such collection via the Privacy Act Notice in tax return instructions.

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

No

Why not?

The legal right to ask for information is IRC sections 6001, 6011, and 6012(a), and their regulations. These sections state that individuals must file a return or statement with IRS for any tax for which they are liable, and response is mandatory.

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

The entire bankruptcy process and procedures are dictated by the Internal Revenue Manual (IRM) guidelines - IRM Part 5.9. IRS policy allows individuals whose data is in the system the opportunity to clarify or dispute negative determinations per the Insolvency Disclosure and Telephone Procedures. Notice, consent, and due process are provided in the tax forms instructions filed by the taxpayer, 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: Administrator

Developers: Read Only

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

IIP utilizes Business Entitlement Access Request System (BEARS) to request access and document approvals for access. Data access is granted on a need-to-know basis. A potential user must submit a request for access to their local management for approval. Users are not permitted access without a signed form from an authorized management official. Specific permissions (Read, Write, Modify, Delete, and/or Print) are defined on the form and set (activated) by the System Administrator prior to the user being allowed access. User privileges and user roles determine the types of data that each user has access to. Management monitors system access and removes permissions when individuals no longer require access.

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 Insolvency Interface Program (IIP) is scheduled under approved NARA Job N1-58-97-13 under AIS as published in Records Control Schedule 35, Item 35. All data meeting end of retention period requirements will be eliminated, overwritten, degaussed, and/or destroyed in accordance with NARA-approved disposition authorities for that system's data, and done so in the most appropriate method based upon the type of storage media used. RCS 32 Item 35: Automated Insolvency System (AIS) master file retention increased from 6 years after case is closed, to 8 years after case is closed for compliance with recordkeeping requirements under the Bankruptcy Abuse Prevention and Consumer Protection Act (BAPCPA).

SA&A OR ASCA

Has the system been through SA&A (Security Assessment and Authorization) or ASCA (Annual Security Control Assessment)?

No

Is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements?

Yes

Describe the system's audit trail.

Batch runs audit trails: They are only kept for 45 days due to space limitations. They are used to troubleshoot problems. Audit trails include: - screen shots of every screen IDRS scanned for data or input to, i.e., FRM77. the flat files that were generated and loaded in the AIS database (DB). Note: these are audit trails of batch runs, there is no user to track. Audit trails of user interactive systems: There is an extensive audit trail of what users do at data entry screens. - When users make a determination at the Automated Discharge System (ADS) module screens, by just entering a one-character code, the userid and date is stored in the AIS DB. All users have access to see this information. - When users mistakenly run a case thru ADS and want the ADS module rows removed, the rows are moved to an audit table (called canc_modu) and the userid and date of the person who requested the move are placed in those moved rows. If a user has access to Ad Hoc reports, they can see this information, or they can ask a programmer to look in the AIS DB for them. - When a user deletes a row (no updates are allowed) from an IIP data file, the data that was deleted and userid and date are stored in an audit file. The file name is "audit_daf". The IIP Administrator can look at this information.

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

IIP is an interface to AIS. In the past AIS has done system test plans that covered IIP.

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: Not Applicable

Contractors: Not Applicable

Members of the Public: Under 100,000

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