Date of Approval: February 19, 2019 PIA ID Number: **3897**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Insolvency Interface Program, IIP

2. Is this a new system? No

2.a. If no, is there a Privacy Civil Liberties Impact Assessment (PCLIA) for this system? Yes

If yes, enter the full name, acronym, and milestone of the most recent PCLIA.

Insolvency Interface Program, IIP, PCLIA #1587

Enter the approval date of the most recent PCLIA. 03/30/2016

If yes Indicate which of the following changes occurred to require this update (check all that apply).

No Addition of Personally Identifiable Information (PII) (PII is any information that is linked or linkable).
No Conversions
No Anonymous to Non-Anonymous
No Significant System Management Changes
No Significant Merging with Another System
No New Access by IRS employees or Members of the Public
No Addition of Commercial Data / Sources
No New Interagency Use
No Internal Flow or Collection
Yes Expiring PCLIA

Were there other system changes not listed above? No

3. What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym.

IIP reports to the Customer Service Domain Change Control Board/Governance Board meeting and elevated items to the Sustaining Operations Executive Steering Committee.

3.a. Check the current Enterprise Life Cycle (ELC) Milestones (select all that apply).

No Vision & Strategy/Milestone 0
No Project Initiation/Milestone 1
No Domain Architecture/Milestone 2
No Preliminary Design/Milestone 3
No Detailed Design/Milestone 4A
Yes System Development/Milestone 4B
No System Deployment/Milestone 5
No Operations & Maintenance (i.e., system is currently operational)

4. Is this a Federal Information Security Management Act (FISMA) reportable system? No

A.1 General Business Purpose

5. 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.

B. PII DETAIL

6. Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any type of Sensitive but Unclassified (SBU) or Personally Identifiable Information (PII)? Yes

6.a. If 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

If yes, check all types of tax identification numbers (TIN) that apply to this system:

Yes	Social Security Number (SSN)
Yes	Employer Identification Number (EIN)
No	Other Taxpayer Identification Number

If SSNs apply, which of the following approved Treasury uses of the SSNs applies:

No	Security background investigations
No	Interfaces with external entities that require the SSN
Yes	Legal/statutory basis (e.g. where collection is expressly required by statute)
Yes	When there is no reasonable alternative means for meeting business requirements
No	Statistical and other research purposes
No	Delivery of governmental benefits, privileges, and services
No	Law enforcement and intelligence purposes
No	Another compelling reason for collecting the SSN

Explain why one or more of the eight authorized uses above support the new or continued use of SSNs.

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 memorandum M-17-12 requires that federal agencies develop a mitigation or elimination strategy for systems that use SSNs. An exception to that requirement is when the SSN is uniquely needed to identify a user's record.

6.b. Does this system use, collect, receive, display, store, maintain, or disseminate other (non-SSN) PII (i.e. Names, addresses, etc.)? Yes

If yes, specify the information.

Selected	PII Element
Yes	Name
Yes	Mailing address
Yes	Phone Numbers
No	E-mail Address
No	Date of Birth
No	Place of Birth
Yes	Standard Employee Identifier (SEID)
No	Mother's Maiden Name
No	Protection Personal Identification Numbers (IP PIN)
No	Internet Protocol Address (IP Address)
No	Criminal History
No	Medical Information
No	Certificate or License Numbers
No	Vehicle Identifiers
No	Passport Number
No	Alien Number
No	Financial Account Numbers
No	Photographic Identifiers
No	Biometric Identifiers
No	Employment Information
Yes	Tax Account Information
No	Centralized Authorization File (CAF)

6.c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? Yes

If yes, select the types of SBU

Selected	SBU Name	SBU Description
Yes	Agency Sensitive Information	Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission
No	Procurement sensitive data	Contract proposals, bids, etc.
Yes	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.
No	Proprietary data	Business information that does not belong to the IRS
Yes	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
No	Physical Security Information	Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities
No	Criminal Investigation Information	Information concerning IRS criminal investigations or the agents conducting the investigations.

6.d. Are there other types of SBU/PII used in the system? No

6.e. Cite the authority for collecting SBU/PII (including SSN if relevant)

Yes PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)

Yes SSN for tax returns and return information is Internal Revenue Code Section 6109

No SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397

No PII for personnel administration is 5 USC

No PII about individuals for Bank Secrecy Act compliance 31 USC

No Information by CI for certain money laundering cases may be 18 USC

6.f. Has the authority been verified with the system owner? Yes

B.1 BUSINESS NEEDS AND ACCURACY

7. 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.

8. How is the SBU/PII verified for accuracy, timeliness, and completeness?

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.

C. 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.

9. 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

If yes, enter the SORN number(s) and the complete the name of the SORN(s).

SORNS Number	SORNS Name
IRS 26.019	Taxpayer Delinquent Account Files
IRS 34.037	Audit Trail and Security Records System

*IRS is required to have a published Privacy Act system of records in the Federal Register. Please identify the Privacy Act SORN(s) that cover these records. If you need additional assistance identifying the correct SORNs please email *Privacy.*

D. RESPONSIBLE PARTIES

10. Identify the individuals for the following system roles. ## Official Use Only

E. INCOMING PII INTERFACES

11. Does the system receive SBU/PII from other system or agencies? Yes

11.a. If yes, does the system receive SBU/PII from IRS files and databases? Yes

If yes, enter the files and databases.

System Name	Current PCLIA	Approval Date	SA&A?	Authorization Date
Integrated Data Retrieval System (IDRS)	Yes	10/01/2018	Yes	01/17/2018
Computer Files On Line (CFOL)	No		No	

11.b. Does the system receive SBU/PII from other federal agency or agencies? No

11.c. Does the system receive SBU/PII from State or local agencies? No

11.d. Does the system receive SBU/PII from other sources? No

11.e. Does the system receive SBU/PII from Taxpayer forms? No

11.f. Does the system receive SBU/PII from Employee forms (such as the I-9)? No

F. DISSEMINATION OF PII

12. Does this system disseminate SBU/PII? Yes

12.a. Does this system disseminate SBU/PII to other IRS Systems? Yes

If yes, identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name	Current PCLIA	Approval Date	SA&A?	Authorization Date
Automated Insolvency System (AIS)	Yes	02/22/2017	Yes	10/02/2015

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.

12.b. Does this system disseminate SBU/PII to other Federal agencies? No

12.c. Does this system disseminate SBU/PII to State and local agencies? No

12.d. Does this system disseminate SBU/PII to IRS or Treasury contractors? No

12.e. Does this system disseminate SBU/PII to other Sources? No

G. PRIVACY SENSITIVE TECHNOLOGY

13. Does this system use social media channels? No

14. Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, Radio Frequency Identification (RFID), etc.? No

15. Does the system use cloud computing? No

16. Does this system/application interact with the public? No

H. INDIVIDUAL NOTICE AND CONSENT

17. Was (or is) notice provided to the individual prior to collection of information? Yes

17.a. If yes, how is notice provided? Was the individual notified about the authority to collect the information, whether such is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects, if any, if they decide not to provide 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.

18. Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information? No

18.b. If individuals do not have the opportunity to give consent, 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.

19. 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.

I. INFORMATION PROTECTION

20. 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

21. The following people have access to the system with the specified rights:

IRS Employees? Yes

IRS Employees?	Yes/No	Access Level (Read Only/Read Write/ Administrator)
Users	Yes	Read and Write
Managers	Yes	Read and Write
Sys. Administrators	Yes	Administrator
Developers	Yes	Read-Only

Contractor Employees? No

21.a. How is access to SBU/PII determined and by whom? Access is determined by need-to-know requirements. User access is given, monitored and removed by Insolvency management through AIS database permissions and roles.

I.1 RECORDS RETENTION SCHEDULE

22. 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

22.a. 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 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.

.

I.2 SA&A OR ASCA

23. Has the system been through Security Assessment and Authorization (SA&A) or Annual Security Control Assessment (ASCA)? No

23.c. If no, is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements? Yes

23.1 Describe in detail 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.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? No

24.b. If no, please explain why. IIP is an interface to AIS. In the past AIS has done system test plans that covered IIP.

K. SBU Data Use

25. Does this system use, or plan to use SBU Data in Testing? No

L. NUMBER AND CATEGORY OF PII RECORDS

26. Identify the number of individual records in the system for each category:
    26.a. IRS Employees: Not Applicable
    26.b. Contractors: Not Applicable
    26.c. Members of the Public: Under 100,000
    26.d. Other: No

M. CIVIL LIBERTIES

27. Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment? No

28. Is the system information used to conduct data-mining as defined in the *Implementing the Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?* No

29. Will this system have the capability to identify, locate, and monitor individuals or groups of people? No

30. Does Computer matching occur? No

N. ACCOUNTING OF DISCLOSURES

31. 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

End of Report