Date of Approval: February 27, 2018 PIA ID Number: 2949

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Standardized IDRS Access Tier II, SIA Tier II

2. Is this a new system? No

2a. If **no**, is there a PIA for this system? Yes

If **yes**, enter the full name, acronym, PIA ID Number and milestone of the most recent PIA.

Standardized IDRS Access Tier II (SIA Tier II) PIA# 475

Next, enter the **date** of the most recent PIA. 12/11/2014

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

No	Addition of PII
No	Conversions
No	Anonymous to Non-Anonymous
No	Significant System Management Changes
Yes	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

Were there other system changes not listed above? No

3. Check the current ELC (Enterprise Life Cycle) 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
Yes	Operations & Maintenance (i.e., system is currently operational)

4. Is this a Federal Information Security Management Act (FISMA) reportable system? Yes

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 Standardized Integrated Data Retrieval System (IDRS) Access Tier II (SIA Tier II) system is used by Current Processing Environment (CPE) and Modernized systems to retrieve IDRS data and to update IDRS and Unisys Master File data. Many projects external to the Unisys systems use SIA Tier II to retrieve taxpayer data, specifically taxpayer identification numbers (TIN), for delivery to either end users of their systems or analysis programs. In addition, these systems external to Unisys systems update IDRS by systemically generating transactions to SIA Tier II. SIA Tier II batch subsystem processing consists of Tier II processes that periodically look for requests from systems that are external to the Unisys systems either in the form of a file that has been sent via File Transfer Protocol (FTP) or as a direct call from those systems that exist on the same SUN Microsystems platform as SIA Tier II, such as Automated Offer in Compromise, (AOIC).

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

6a. 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 who the SSN (or tax identification number) is collected on.

Yes On Primary Yes On Spouse Yes On Dependent

If **yes**, check all types SSN s (or tax identification numbers) that apply to this system:

Yes Social Security Number (SSN)
Yes Employer Identification Number (EIN)
Yes Individual Taxpayer Identification Number (ITIN)
Yes Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
Yes Practitioner Tax Identification Number (PTIN)

Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN s (or tax identification numbers).

There is no known mitigation strategy planned to eliminate the use of SSN for the system; SSN is required for the use of this system. The SSN number is needed to research and locate records in response to the request.

6b. Does this system contain other (non-SSN) PII that it uses, collects, receives, displays, stores, maintains, or disseminates? (i.e. Names, addresses, etc.) Yes

If **yes**, specify the information.

Selected	PII Element	On Primary	On Spouse	On Dependent
Yes	Name	Yes	No	No
Yes	Mailing address	No	No	No
Yes	Phone Numbers	No	No	No
Yes	E-mail Address	No	No	No
Yes	Date of Birth	Yes	Yes	Yes
No	Place of Birth	No	No	No
No	SEID	No	No	No
No	Mother's Maiden Name	No	No	No
No	Protection Personal Identification Numbers (IP PIN)	No	No	No
No	Internet Protocol Address (IP Address)	No	No	No
No	Criminal History	No	No	No
No	Medical Information	No	No	No
No	Certificate or License Numbers	No	No	No
No	Vehicle Identifiers	No	No	No
No	Passport Number	No	No	No
No	Alien (A-) Number	No	No	No
No	Financial Account Numbers	No	No	No
No	Photographic Identifiers	No	No	No
No	Biometric Identifiers	No	No	No
No	Employment (HR) Information	No	No	No
Yes	Tax Account Information	Yes	No	No

6c. 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
No	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
No	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.

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

6e. 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

6f. 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.

SIA Tier II follows the concept of least privilege, and access controls are implemented according to IRM 10.8.1 to protect the confidentiality and integrity of information at rest; application administrator can only access information necessary to perform their job function. The application adheres to the Security Assessment and Authorization (SA&A) and physical security requirements set forth in IRM 10.4.1- Physical Security Program- Managers Security Handbook.

8. How is the SBU/PII verified for accuracy, timeliness, and completeness? Explain how steps are taken to ensure that all information maintained by the system that is used by IRS to make any adverse determination about an individual's rights, benefits, and/or privileges is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination

SIA Tier II uses only PII data that has been previously validated by the system providing the data; the data received are from trusted internal IRS sources and are assumed accurate upon receipt. It is the responsibility of the Tier 1 systems to verify the data for accuracy, timeliness, and completeness. Timeliness of data is taken care of by the proper scheduling when SIA Tier I batch extract applications are run. Data extracts sent to SIA Tier II applications occur after all daily/weekly updates to IDRS are completed. Data refresh requests may be made as needed.

C. PRIVACY ACT AND SYSTEM OF RECORDS

9. Are 10 or more records containing SBU/PII maintained, stored, and/or transmitted by or through this system? Yes

9a. If **yes**, are records in the system retrieved by any personal identifier (e.g., name, SSN, Photograph, IP Address) for an individual? Yes

If **yes**, is there a System of Records Notice(s) or SORNs that addresses the PII records in this system? Yes

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

SORNS Number	SORNS Name
Treasury/IRS 24.030	Individual Master File
Treasury/IRS 24.046	Business Master File
Treasury/IRS 26.009	Lien Files
Treasury/IRS 26.012	Offer in Compromise File
Treasury/IRS 26.019	Taxpayer Delinquent Account Files
Treasury/IRS 34.037	IRS Audit Trail and Security Records System

If **yes**, does the System of Records Notice(s) (SORN) published in the Federal Register adequately describe the records as required by the Privacy Act? Yes

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

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

If **yes**, enter the files and databases.

System Name	Current PIA?	PIA Approval Date	SA & A?	Authorization Date
Taxpayer Delinquent Account (TDA)	Yes	07/12/2011	Yes	12/09/2011
Automated Collection System (ACS)	Yes	12/11/2012	Yes	05/25/2010
Automated Liens System - Entity Case Management System (ALS-Entity)	Yes	11/12/2013	Yes	03/23/2011
Automated Offers in Compromise (AOIC)	Yes	06/29/2012	Yes	09/28/2009
Automated Substitute for Return (ASFR)	Yes	01/20/2014	Yes	06/06/2011
Integrated Collection System (ICS)	Yes	09/19/2013	Yes	05/19/2011
Automated 6020(b) Substitute for Returns (A6020b)	Yes	07/27/2012	Yes	07/16/2010

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

If **yes**, for each federal interface, identify the organization that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA)/Memorandum of Understanding (MOU).

Organization Name	Transmission method	ISA/MOU
Social Security Administration	eTransmittal	Yes

11c. Does the system receive SBU/PII from State or local agencies? Yes

If **yes**, for each state and local interface identify the organization that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name	Transmission method	ISA/MOU
All US State Tax Agencies	eTransmittal	Yes

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

11e. Does the system receive SBU/PII from **Taxpayer** forms? Yes

If **yes**, identify the forms

Form Number	Form Name
1040	U.S. Individual Income Tax Return
1065	Return of Partnership Income
1120	U.S. Corporation Income Tax Return
941	Employer's Quarterly Federal Tax Return
940	Employer's Annual Federal Unemployment (FUTA) Tax Return
990	Return of Organization Exempt from Income Tax
720	Quarterly Federal Excise Tax Return
1041	U.S. Income Tax Return for Estates and Trusts
706	United States Gift (and Generation - Skipping Transfer) Tax Return

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

F. PII SENT TO EXTERNAL ORGANIZATIONS

12. Does this system disseminate SBU/PII? Yes

12a. 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 PIA?	PIA Approval Date	SA & A?	Authorization Date
Notice Delivery System (NDS)	Yes	01/08/2013	Yes	05/13/2010
Inventory Delivery System (IDS)	Yes	01/15/2014	Yes	05/01/2009
Taxpayer Delinquent Account (TDA)	Yes	07/12/2011	Yes	12/09/2011
Automated Collection System (ACS)	Yes	12/11/2011	Yes	05/25/2011
Automated Substitute for Return (ASFR)	Yes	01/29/2014	Yes	06/06/2011
Automated 6020(b) Substitute for Returns (A6020b)	Yes	07/27/2012	Yes	07/16/2010
Automated Liens System - Entity Case Management System (ALS-Entity)	Yes	11/12/2013	Yes	03/23/2013
Automated Offers in Compromise (AOIC)	Yes	06/29/2012	Yes	09/28/2009

Identify the authority and for what purpose? Authorities: OMB M 03-22 & Internal Revenue Manual (IRM) 10.8.8, IT Security, Live Data Protection Policy & PVR #16, Acceptable Use.

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

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

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

12e. 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, RFID, etc.? No

15. Does the system use cloud computing? Yes

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

H. INDIVIDUAL NOTICE AND CONSENT

17. Was/is notice provided to the individual prior to collection of information? Yes

17a. 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 individual is 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, are decide not to provide any of the requested information, when required. Notice is provided in the tax return instructions.

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

18a. If **yes**, describe the mechanism by which individuals indicate their consent choice(s):
SIA Tier II uses only PII data that has been previously validated by the system providing the data; the data received are from trusted internal IRS sources and are assumed accurate upon receipt. It is the responsibility of the Tier 1 systems to verify the data for accuracy, timeliness, and completeness.

19. How does the system or business process ensure due process regarding information access, correction and redress?
Taxpayers receive appeal rights Per Title 26 USC.

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-Only
Managers	Yes	Read-Only
Sys. Administrators	Yes	Administrator
Developers	Yes	Administrator

Contractor Employees? Yes

Contractor Employees?	Yes/No	Access Level	Background Invest. Level
Contractor Users	Yes	Read-Only	Moderate
Contractor Managers	No		
Contractor Sys. Admin.	Yes	Administrator	High
Contractor Developers	Yes	Administrator	High

21a. How is access to SBU/PII determined and by whom? SIA Tier II follows the concept of least privilege, and access controls are implemented according to IRM 10.8.1 to protect the confidentiality and integrity of information at rest; application administrator can only access information necessary to perform their job function. The application adheres to the SA&A and physical security requirements set forth in IRM 10.4.1- Physical Security Program- Managers Security Handbook. SIA Tier II uses only PII data that has been previously validated by the system providing the data; the data received are from trusted internal IRS sources and are assumed accurate upon receipt. It is the responsibility of the Tier 1 systems to verify the data for accuracy, timeliness, and completeness. Timeliness of data is taken care of by the proper scheduling when SIA Tier I batch extract applications are run. Data extracts sent to SIA Tier II applications occur after all daily/weekly updates to IDRS are completed. Data refresh requests may be made as needed.

21b. If computer matching occurs, can the business owner certify that it meets requirements of IRM 11.3.39 Disclosure of Official Information, Computer Matching & Privacy Protection Act? Yes

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? No

22b. 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.

In the determination of the Service-wide Records Officer, IRS Records and Information Management Program, data contained in the Integrated Data Retrieval System is non-record and therefore not subject to disposition and records retention requirements codified in 36 CFR Chapter XII (requiring final disposition approval from the Archivist of the United States). The SIA Tier II application deletes all files once they reach the predefined retention period of one month, as specified by Internal Revenue Manual 10.8.1 - Information Technology (IT) Security, Policy and Guidance. Data is deleted from the database on a daily basis once the data is no longer needed to validate a transaction. Files are retained by SIA for a sufficient period of time to allow transactions to post to IDRS and Master File and time for the business to verify all transactions have been applied to IDRS and Master File. This retention also provides sufficient time for a rapid recovery in case of an application problem, a system problem or disaster problem.

I.2 SA&A OR ECM-R

23. Has the system been through SA&A (Security Assessment and Authorization) or ECM-R (Enterprise Continuous Monitoring Reauthorization)? No

23c. 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. There are no regular end user activities on the SIA Tier II application, so there are no auditable events to capture on end users. The application administrator has UNIX base access account and the system administrators have infrastructure accounts; they are audited at the operating system level. Auditing at the SIA Tier II application level is thus not applicable. All SIA Tier II auditing is performed at the infrastructure level by the Modernization & Information Technology Services (MITS)-24 General Support System (GSS).

J. PRIVACY TESTING

24. Does the system require a System Test Plan? Yes

24b. If **yes**, Is the test plan in process or completed: Completed

24.3 If **completed/ or in process,** describe what testing and validation activities have been conducted or are in progress to verify and validate that the applicable Privacy Requirements (listed in header) have been met?
This Information System Contingency Plan (ISCP) Testing is prepared by Disaster Recovery Testing & Business Analysis (DRTBA) for use by all Business Operating Divisions (BODs) to inform BOD participants about the activities required to perform ISCP Tabletop and Functional Exercises and testing during the current FISMA reporting cycle and is designed to assist BODs as they monitor and track the activities of each phase of the ISCP and Analysis Specification Package (ASP) testing process to ensure that they meet all FISMA requirements for annual ISCP testing. Monthly RA-5 Vulnerability Scan are conducted to monitor and address the results from the scans on databases, applications, software/hardware.

24b.1. If **completed**, where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)? Test plan results are stored on share drives for each business unit.

24b.2. If **completed**, were all the Privacy Requirements successfully tested? Yes

24.2 If **completed**, are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved? No

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:

26a. IRS Employees: More than 100,000
26b. Contractors: Not Applicable
26c. Members of the Public: More than 1,000,000
26d. 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 9/11 Commission Recommendations 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? Yes

If **yes**, describe the type of information derived from these efforts and the technical (e.g., audit trails) or other processes used to limit unauthorized monitoring. IRS Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program (1) To implement the requirements of the Taxpayer Browsing Protection Act of 1997 (Public Law No. 105-35), the IRS created the unauthorized access, attempted access or inspection of taxpayer records (UNAX) program. The Taxpayer Browsing Protection Act, in conjunction with the UNAX program, provides the following: Willful unauthorized access or inspection of taxpayer records is a crime, punishable upon conviction, by fines, imprisonment, and termination of employment. Taxpayer records include hard copies of returns and return information, as well as returns and return information maintained on a computer; A taxpayer who is a victim of unlawful access or inspection has the right to take legal action even if the taxpayer's information is never revealed to a third party; When IRS employees are criminally charged, the IRS is required to notify taxpayers that their records have been accessed without authorization; For contractors, the willful unauthorized access or inspection of taxpayer records can carry penalties upon conviction of removal from the contract, fines, and imprisonment; Criminal UNAX violations result from intentional unauthorized inspection of returns and return information. Under 26 USC 7213A, the violation is punishable by a fine not to exceed $1,000 or imprisonment of not more than 1 year, or both, together with the costs of prosecution. Upon conviction, the employee is terminated; Non-Criminal Penalties – pursuant to IRS UNAX policy, removal is to be proposed for all UNAX violations. The penalty can be mitigated to suspension by the deciding official at the decision stage; and UNAX can lead to additional criminal charges such as falsification of records, fraud, embezzlement and identity theft. (2) IRS UNAX Policy provides that employees may be subject to administrative penalties for the willful and unauthorized attempted access of their own or another taxpayer's records. Administrative penalties include: Removal of employee Suspension of employee Additional information on penalties for UNAX violations can be found in the Guide to Penalty

Determinations. http://publish.no.irs.gov/getpdf.cgi?catnum=32178 (3) The IRS relies on the ethics and integrity of its employees and contractors and enlists their support in eliminating all cases of UNAX. Employees who have knowledge of a suspected UNAX violation, must report to the U.S. Treasury Inspector General for Tax Administration (TIGTA), or their managers.

N. ACCOUNTING OF DISCLOSURES

30. 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? Yes

    If **yes**, does the system have a process in place to account for such disclosures in compliance with IRC 6103 (p) (3) (A) or Subsection (c) of the Privacy Act? Contact *Disclosure* to determine if an accounting is required. Yes

End of Report