Date of Approval: **May 04, 2023**

PIA ID Number: **7329**

SYSTEM DESCRIPTION

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

Standardized IDRS Access Tier II, SIA Tier II

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?

Standardized IDRS Access Tier II (SIA Tier II) PIA# 2949

What is the approval date of the most recent PCLIA?

2/27/2018

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.

Enterprise Computing Center Change Control Board (ECC CCB)

Current ELC (Enterprise Life Cycle) Milestones:

System Development/Milestone 4B

Operations & Maintenance (i.e., system is currently operational)

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

Yes

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 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).

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).

SSN is required for the use of this system. The SSN number is needed to research and locate records in response to the request.

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.

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
E-mail Address
Date of Birth
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:

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.

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.

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.

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

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.

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 24.030 Customer Account Data Engine Individual Master File

IRS 24.046 Customer Account Data Engine Business Master File

IRS 26.009 Lien Files

IRS 26.012 Offer in Compromise Files

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: Automated Collection System (ACS)
Current PCLIA: Yes
Approval Date: 10/1/2021
SA&A: Yes
ATO/IATO Date: 12/1/2021

System Name: Automated Liens System - Entity Case Management System (ALS-Entity)
Current PCLIA: Yes
Approval Date: 9/24/2021
SA&A: Yes
ATO/IATO Date: 3/28/2021

System Name: Automated Offers in Compromise (AOIC)
Current PCLIA: Yes
Approval Date: 5/3/2021
SA&A: Yes
ATO/IATO Date: 9/30/2020

System Name: Taxpayer Delinquent Account (TDA)
Current PCLIA: Yes
Approval Date: 10/26/2021
SA&A: Yes
ATO/IATO Date: 11/1/2021

System Name: Automated Substitute for Return (ASFR)
Current PCLIA: Yes
Approval Date: 12/6/2019
SA&A: Yes
ATO/IATO Date: 7/15/2019

System Name: Integrated Collection System (ICS)
Current PCLIA: Yes
Approval Date: 3/7/2022
SA&A: Yes
ATO/IATO Date: 2/23/2019

System Name: Automated 6020(b) Substitute for Returns (A6020b)
Current PCLIA: Yes
Approval Date: 9/17/2021
SA&A: Yes
ATO/IATO Date: 5/23/2021

System Name: Combined Fed State
Current PCLIA: Yes
Approval Date: 4/6/2020
SA&A: No

System Name: Individual Master File (IMF)
Current PCLIA: Yes
Approval Date: 3/4/2020
SA&A: Yes
ATO/IATO Date: 11/26/2019

System Name: Taxpayer Delinquent Account (TDA)
Current PCLIA: Yes
Approval Date: 10/26/2021
SA&A: Yes
ATO/IATO Date: 11/1/2021

System Name: Inventory Delivery System (IDS)
Current PCLIA: Yes
Approval Date: 11/22/2019
SA&A: Yes
ATO/IATO Date: 11/1/2015

System Name: Automated Manual Assessments (AMA)
Current PCLIA: Yes
Approval Date: 4/26/2021
SA&A: Yes
ATO/IATO Date: 10/14/2020

System Name: Information Returns Processing (IRP)
Current PCLIA: Yes
Approval Date: 3/16/2020
SA&A: Yes
ATO/IATO Date: 10/22/2015

System Name: Locator Services System (LSS)
Current PCLIA: Yes
Approval Date: 3/30/2021
SA&A: Yes
ATO/IATO Date: 11/26/2019

System Name: National Account Profile (NAP)
Current PCLIA: Yes
Approval Date: 2/27/2020
SA&A: No

System Name: Notice Delivery System (NDS)
Current PCLIA: Yes
Approval Date: 8/3/2020
SA&A: Yes
ATO/IATO Date: 11/13/2018

System Name: SIATIER1
Current PCLIA: Yes
Approval Date: 2/27/2018
SA&A: No

System Name: Business Master File (BMF)
Current PCLIA: Yes
Approval Date: 9/22/2021
SA&A: Yes
ATO/IATO Date: 11/12/2020

System Name: Taxpayer Delinquent Investigation (TDI)
Current PCLIA: Yes
Approval Date: 10/26/2021
SA&A: Yes
ATO/IATO Date: 11/1/2021

Does the system receive SBU/PII from other federal agency or agencies?

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).

Name: Social Security Administration
Transmission Method: eTransmittal
ISA/MOU: Yes

Does the system receive SBU/PII from State or local agency (-ies)?

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: All US State Tax Agencies
Transmission Method: eTransmittal
ISA/MOU: Yes

Does the system receive SBU/PII from other sources?

No

Does the system receive SBU/PII from Taxpayer forms?

Yes

Please identify the form number and name:

Form Number: 1040
Form Name: U.S. Individual Income Tax Return

Form Number: 1065
Form Name: Return of Partnership Income

Form Number: 1120
Form Name: U.S. Corporation Income Tax Return

Form Number: 941
Form Name: Employer's Quarterly Federal Tax Return

Form Number: 940
Form Name: Employer's Annual Federal Unemployment (FUTA) Tax Return

Form Number: 990
Form Name: Return of Organization Exempt From Income Tax

Form Number: 720
Form Name: Quarterly Federal Excise Tax Return

Form Number: 1041
Form Name: U.S. Income Tax Return for Estates and Trusts

Form Number: 706
Form Name: United States Gift (and Generation - Skipping Transfer) Tax Return

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: Notice Delivery System (NDS)
Current PCLIA: Yes
Approval Date: 8/3/2020
SA&A: Yes
ATO/IATO Date: 11/13/2018

System Name: Inventory Delivery System (IDS)
Current PCLIA: Yes
Approval Date: 1/15/2014
SA&A: Yes
ATO/IATO Date: 5/1/2009

System Name: Taxpayer Delinquent Account (TDA)
Current PCLIA: Yes
Approval Date: 10/26/2021
SA&A: Yes
ATO/IATO Date: 11/1/2021

System Name: Automated Collection System (ACS)
Current PCLIA: Yes
Approval Date: 10/1/2021
SA&A: Yes
ATO/IATO Date: 12/1/2021

System Name: Automated Substitute for Return (ASFR)
Current PCLIA: Yes
Approval Date: 12/6/2019
SA&A: Yes
ATO/IATO Date: 7/15/2019

System Name: Automated 6020(b) Substitute for Returns (A6020b)
Current PCLIA: Yes
Approval Date: 9/17/2021
SA&A: Yes
ATO/IATO Date: 5/23/2021

System Name: Automated Liens System - Entity Case Management System (ALS-Entity)
Current PCLIA: Yes
Approval Date: 9/24/2021
SA&A: Yes
ATO/IATO Date: 3/28/2021

System Name: Automated Offers in Compromise (AOIC)
Current PCLIA: Yes
Approval Date: 5/3/2021
SA&A: Yes
ATO/IATO Date: 9/30/2020

System Name: Automated Manual Assessments (AMA)
Current PCLIA: Yes
Approval Date: 4/26/2021
SA&A: Yes
ATO/IATO Date: 10/14/2020

System Name: Business Master File (BMF)
Current PCLIA: Yes
Approval Date: 9/22/2021
SA&A: Yes
ATO/IATO Date: 11/12/2020

System Name: Combined Fed State
Current PCLIA: Yes
Approval Date: 4/6/2020
SA&A: No

System Name: Integrated Collection System (ICS)
Current PCLIA: Yes
Approval Date: 3/7/2022
SA&A: Yes
ATO/IATO Date: 2/23/2019

System Name: Individual Master File (IMF)
Current PCLIA: Yes
Approval Date: 3/4/2020
SA&A: Yes
ATO/IATO Date: 11/26/2019

System Name: Information Returns Processing (IRP)
Current PCLIA: Yes
Approval Date: 3/16/2020
SA&A: Yes
ATO/IATO Date: 10/22/2015

System Name: Taxpayer Delinquent Account (TDA)
Current PCLIA: Yes
Approval Date: 10/26/2021
SA&A: Yes
ATO/IATO Date: 11/1/2021

System Name: Taxpayer Delinquent Investigation (TDI)
Current PCLIA: Yes
Approval Date: 10/26/2021
SA&A: Yes
ATO/IATO Date: 11/1/2021

System Name: Locator Services System (LSS)
Current PCLIA: Yes
Approval Date: 3/30/2021
SA&A: Yes
ATO/IATO Date: 11/26/2019

System Name: National Account Profile (NAP)
Current PCLIA: Yes
Approval Date: 2/27/2020
SA&A: No

System Name: Notice Delivery System (NDS)
Current PCLIA: Yes
Approval Date: 8/3/2020
SA&A: Yes
ATO/IATO Date: 11/13/2018

System Name: SIATIER1
Current PCLIA: Yes
Approval Date: 2/27/2018
SA&A: No

Identify the authority.

Authorities: OMB M 03-22 & Internal Revenue Manual (IRM) 10.8.8, IT Security, Live Data Protection Policy & PVR #16, Acceptable Use.

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.

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 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.

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

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.

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

Taxpayers receive appeal rights Per Title 26 USC -. United States Code

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 Only
Managers: Read Only
System Administrators: Administrator
Developers: Administrator

IRS Contractor Employees

Contractor Users: Read Only
Contractor System Administrators: Administrator

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

SIA Tier II is a batch system process. There are no users and no user interface. Anyone requiring access to the system must request a firecall account. This is only granted in exceptional circumstances and only after managerial approval of a BEARS request.

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?

No

You must work with the IRS Records and Information Management (RIM) Program Office to address records retention requirements before you dispose of any records in this system.

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.

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).

PRIVACY TESTING

Does the system require a System Test Plan?

Yes

Is the test plan completed?

Yes

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.

Were all the Privacy Requirements successfully tested?

Yes

Are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved?

No

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 Federal Information Security Management Act (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.

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: More than 100,000

Contractors: Not Applicable

Members of the Public: More than 1,000,000

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?

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.

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?

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