

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: December 17, 2014

PIA ID Number: **475**

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):

Standardized IDRS Access Tier II, SIA Tier II

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: Not Applicable

Number of Contractors: Not Applicable

Members of the Public: Not Applicable

4. Responsible Parties:

NA

5. General Business Purpose of System

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).

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: 6/7/2012 12:00:00 AM

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

SIA Tier II codes had to be modified to accommodate the conversion from Oracle 10g to 11g.

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'. 015-45-01-11-01-2218-00

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
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 Yes
 Employees/Personnel/HR Systems No

Other No

Other Source: _____

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

Additional Types of PII: Yes

<u>PII Name</u>	<u>On Public? On Employee?</u>	
EIN	Yes	No
taxpayer telephone number	Yes	No

- 10a. What is the business purpose for collecting and using the SSN ?
 Assist in the collection of taxes

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.)
 SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns. Additional information can be found at these two links:
<http://www.irs.gov/pub/irs-wd/00-0075.pdf> <http://www.law.cornell.edu/uscode/text/26/6109>

- 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 alternate solution has been considered. The SIA Tier II system uses the TIN as the personal identifier within the system. The TIN is employed as part of a unique key used to identify input and output of SIA Tier II data. This personal identifier cannot be eliminated or minimized by using another personal identifier.

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

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.

Describe the PII available in the system referred to in question 10 above.

PII data available in the SIA Tier II system are those of taxpayers and includes SSNs, TINs, address, EIN, and Telephone number.

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.

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 MITS-24 GSS.

11a. Does the audit trail contain the audit trail elements as required in current IRM 10.8.3 *Audit Logging Security Standards*? No

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:

<u>System Name</u>	<u>Current PIA?</u>	<u>PIA Approval Date</u>	<u>SA & A?</u>	<u>Authorization Date</u>
Automated Offers in Compromise (AOIC)	Yes	06/29/2012	Yes	09/28/2009
Integrated Collection System (ICS)	Yes	09/19/2013	Yes	05/19/2011
Inventory Delivery System (IDS)	Yes	01/15/2014	Yes	05/01/2009
Standard IDRS Access Tier II	No	01/15/2014	No	05/01/2009
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
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	01/29/2014	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
Notice Delivery System (NDS)	Yes	01/08/2013	Yes	05/03/2010
Inventory Delivery System (IDS)	Yes	01/15/2014	Yes	05/01/2009
Automated 6020(b) Substitute for Returns (A6020b)	Yes	07/27/2012	Yes	07/16/2010
Automated Substitute for Return (ASFR)	Yes	01/29/2014	Yes	06/06/2011
Notice Delivery System (NDS)	Yes	01/08/2013	Yes	05/03/2010

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.) No

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)			
State and local agency (-ies)			
Third party sources			
Other:			

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

16. Does this system host a website for purposes of interacting with the public? No

17. Does the website use any means to track visitors' activity on the Internet?

If yes, please indicate means:

	YES/NO	AUTHORITY
Persistent Cookies	_____	_____
Web Beacons	_____	_____
Session Cookies	_____	_____
Other:	_____	_____

If other, specify:

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? Not Applicable

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? Yes

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

The system will allow affective parties the opportunity to clarify or dispute negative information that could be used against them. Due process is provided pursuant to 5 USC.

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>Yes</u>
Other:	<u>No</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>No</u>	
Users		_____
Managers		_____
System Administrators		_____
Developers		_____
Contractors:	<u>No</u>	
Contractor Users		_____
Contractor System Administrators		_____
Contractor Developers		_____
Other: <u>application administrators</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?

23. How is access to the PII determined and by whom?

There are no regular end users accessing the SIA Tier II system. The SIA Tier II system has one application administrator who has access right to the application. The application administrator account is granted access on the SIA Tier II system through the use of OL5081 process, which requires management approval. This access account is a role base UNIX account; the MITS-24 GSS system administrator created the restricted access role to allow the application administrator to perform specific monitoring functions of the health and well-being of the SIA Tier II system.

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

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.

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? No

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.

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 bases 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.

26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.

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.

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

All internal to the IRS

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.

SIA Tier II stakeholders meet prior to any major change being made to the SIA Tier II application or system environment. Before changes are made, they are evaluated against the business requirements, which are generated and approved by application stakeholders. Specific planning and coordination occurs before conducting security-related activities affecting the information system. Appropriate planning and coordination between MITS Cybersecurity, the MITS Certification Program Office (CPO), MITS IT Security Architecture and Engineering (ITSAE), and the SIA Tier II Stakeholders occur before conducting these activities to minimize the impact on the SIA Tier II operations. On an annual basis, the business unit participates in the Enterprise Continuous Monitoring Exercises, including updates to the Information Security Contingency Plan (ISCP) and SSP. Every three years, SIA Tier II will go through the SA&A process, which, in addition to the annual exercises, includes a comprehensive Security Control Assessment (SCA). When security audits, Security Control Assessment (SCA)'s, Security Impact Assessments (SIA), Security Risk Assessments (SRA) or certification activities are required, the Security PMO, MITS Security Assessment Services (SAS) and MITS Cybersecurity communicate with the Business Unit to ensure that they understand the scope of the security activity to be conducted.

29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 - *IT Security, Live Data Protection Policy*? Not Applicable

29a. Has approval been received from the Office of Privacy Compliance to use Live Data in testing (*if appropriate*)?

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

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.

SORN Number	SORN 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

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:

N. A.