

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: April, 9 2014 12:00AM

PIA ID Number: **822**

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):

Integrated Submission Remittance Processing, ISRP

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: Under 50,000

Number of Contractors: Under 5,000

Members of the Public: Not Applicable

4. Responsible Parties:

NA

5. General Business Purpose of System

ISRP is a major application designed to capture, format, and forward information related to tax submissions and remittances in electronically readable formats to downstream IRS systems. ISRP is owned and operated by the Wage and Investment (W&I) Business Unit (BU) and is comprised of two main functions which include Submission Processing and Remittance Processing. Submission Processing – is the component of ISRP that captures and formats tax documents into electronic data for export to other IRS systems. Submission Processing is used to transcribe data from paper tax documents into an electronic format that can be read by other IRS systems. ISRP supports all IRS Tax forms. When a tax document is received, it is opened and sorted by form type (e.g., Form 1040 and Form 1040A, etc.) by mailroom operations, who then forward to ISRP. Any remittances received with a tax document are forwarded and processed for deposit to the Remittance Processing function and separated from the tax document. Tax documents are sorted by form type and placed into groups of 100 documents or less, called blocks. When a block enters Submission Processing, it is selected by an Entry Operator (EOP), who enters the tax data for the block into the ISRP system using the Original Entry (OE) operation. Once OE is completed for a block, the block is then moved to Key Validation (KV), where the tax data is re-entered. Any information entered in KV that differs from the data that was entered during OE requires re-entry for verification. Once a block completes KV, it is available for formatting. During OE, entered data which identifies the taxpayer can be verified, if necessary, against the Enhanced Entity Index File (E-EIF) database to determine if additional entity information is required to be entered by the EOP. Block Edit (BE) allows an EOP to review and edit previously entered blocks. It allows a Quality Review (QR) operator to review data, and if the system configuration allows, to edit data. After the block completes verification, the data is formatted and held for the End of Shift (EOS) process where the data is exported via the Enterprise File Transfer Utility (EFTU) which transfers the data files to the Unisys Mainframe [Modernization & Information Technology Services (MITS-23) located either at the Enterprise Computing Center - Martinsburg (ECC-MTB) or the Enterprise Computing Center – Memphis (ECC-MEM) depending upon the location of the ISRP campus. The actual file transfer is a “store and forward” implementation which is triggered by a Work Order (WO) received by EFTU from ISRP by a pre-scheduled scan of a predetermined folder on ISRP. EFTU validates the request and then issues a separate request to ISRP to retrieve the data files. The EFTU control server receives files from ISRP which are transmitted via Tectia Secure Shell (SSH) and then EFTU transmits the files to the Unisys mainframe (MITS-23). During all phases of Submission Processing, ISRP maintains a dynamic database tracking the blocks being processed, their status in submission processing, and operator statistics in the Inventory and Operator Statistics (OPSTATS) databases. For each Revenue Receipts transaction transcribed, a record of that transaction along with an identifying deposit trace number is created for the Custodial Detail Database (CDDDB). At the EOS, a data file is exported via EFTU which then transfers the data file to the CDDDB system. This information is used by the Chief Financial Officer (CFO) to track all transactions that relate to “deposit of money in the IRS.” Remittance Processing – is the component of ISRP that

captures and formats remittance data for export to other IRS systems. Remittance Processing is a multifunctional process which automates the control of taxpayer documents and the deposit of associated remittances and includes an OE/KV function and a Remittance Scanning Function. OE/KV As in Submission Processing, when a tax document is received, it is opened and sorted by form type (e.g., 1040, 1040A, etc.) by mailroom operations, who then forward to ISRP. Prior to entering Remittance Processing, remittances with their accompanying documentation are pre-sorted into groups called "Batches." A remittance that is to be applied to a single tax account and that is accompanied by a single paper voucher is sorted into a Remittance Voucher (RV) Batch of up to 300 remittances. RV Batches are not processed by OE, but are instead separated from the rest of the submission and processed for deposit immediately through the Remittance Scanning Function. A remittance not accompanied by a voucher that is to be applied to a single tax account is sorted into an OE/KV Batch of up to 100 remittances. The OE process consists of retrieving batches of remittances with associated tax documents and then control document data, tax form data, and associated remittance amounts are manually captured into fields on a template for the purpose of creating an electronic voucher. The EOP enters the Remittance Processing System Identification Number (RPSID). The system assigns a serial number to each remittance within the batch. Then the operator enters the remittance data into fields on a template. A function is provided which allows the operator to reject a remittance if any necessary information [i.e., Taxpayer Identification Number (TIN), Master File Tax Code (MFT), TIN Type, etc.] are not available, or if the remittance is incorrectly made out. Work that has been processed through OE is then placed back onto the batch cart so that it can then be processed through KV. The KV process consists of retrieving batches of remittances with associated tax documents previously entered into Remittance Processing by the OE EOP and re-entering the data. Any discrepancies are flagged by the Remittance Processing system. Problem documents encountered are routed back to Pre-batch. The remittances are separated from the accompanying tax documentation, which is removed from the Remittance Processing system and returned to the batch cart. The completed electronic vouchers and remittances are routed to the Transport System (Unisys NDP600). Remittance Scanning Remittance Scanning is handled through the Transport System (Unisys NDP600), an industrial scanning system used to scan remittance (checks, money orders, vouchers) data through two passes. After mail sorting, the paper voucher "Singles" transactions are processed on the Transport System to capture the voucher scan line information and images, and to capture the remittance Magnetic Ink Character Recognition (MICR) scan line information and images. The Optical Character Recognition (OCR) reader reads vouchers prepared with the OCR-A or the OCR-B font on the Transport System. The Intelligent Character Recognition (ICR) engine reads vouchers prepared with the Courier 10 font immediately after Pass 1. The images of items containing "can't reads" or items with missing fields are forwarded to data entry. On Pass 2, the Transport System includes a scan for item verification, endorsement with the IRS Stamp and audit trail, encoding the amount on the check, imaging, and sorting. Based on the information read from the batch header ticket, the system uploads the database information from the remittance processing database to the Transport System. The MICR information is read from the checks and compared to the information captured during Pass 1. This is done to automatically identify and verify the item. If the information does not match, the operator must match the item to the list of unprocessed items that appears on screen or reject it. If the information does match, the item is endorsed, encoded, imaged, and sorted according to the parameters in the sort pattern. Remittances and associated deposit reports are packaged for presentation to the bank and then sent via registered courier to participating banking institutions (banks) for deposit. Once processed through Remittance Processing, the electronic data is held until the End Of Day (EOD) process then is exported via EFTU which transfers the data files the same way as in Submission Processing to the Unisys Mainframe (MITS-23) located either at ECC-MTB or ECC-MEM, again depending upon the location of the ISRP campus. Also as in Submission Processing, the actual file transfer is a "store and forward" implementation which is triggered by a WO received by EFTU from ISRP. EFTU validates the request and then issues a separate request to ISRP to retrieve the data files. The EFTU control server receives files from ISRP which are transmitted via Tectia SSH to EFTU which then transmits the files to the Unisys mainframe (MITS-23). For each remittance transaction processed, a record of that transaction along with an identifying deposit trace number is created for the CDDB. At the EOD, a data file is exported via EFTU where it is transferred to the CDDB. This information is used by the CFO to track all transactions that relate to "deposit of money" in the IRS. In addition, ISRP uses EFTU to transfer remittance data to the Remittance Transaction Research (RTR) system located at ECC-MEM. The ISRP RTR utility running on the ISRP Export PC converts RTR data into an eXtensible Markup Language (XML) file. The MultiImageBuilder service, executing on an ISRP Application Server, continuously polls the system for completed batches. When a batch is completed, the images for that batch are retrieved and formatted into a Multi-Image Tagged Image File Format (TIFF) file. The data in the XML and TIFF files are validated using validation rules. After validation, the files are compressed and transmitted via Tectia SSH to EFTU which then forwards this data to the RTR system. Due process is provided pursuant to 26 USC.

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: 04/27/2011

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 No

6c. State any changes that have occurred to the system since the last PIA
No changes this PIA is being completed due to the three year expiration.

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'. N/A

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

8a. If **No**, what types of information does the system collect, display, store, maintain or disseminate?

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	<u>Yes</u>	
Employees/Personnel/HR Systems	<u>Yes</u>	
Other	<u>Yes</u>	<u>Other Source:</u> <u>Audit Trail</u>

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	Yes	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: No

PII Name On Public? On Employee?

No No

10a. What is the business purpose for collecting and using the SSN ?

The ISRP application includes taxpayer data elements and fields from over 200 paper tax forms (i.e. 1040, 1040A, 1040EZ, 1120) and taxpayer checks for forwarding to downstream IRS systems for processing.

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.)

IRC 6109(a) IRM 10.2.1.4 IRC 6103, 7213, 7217 and 7431

10c. What alternative solution to the use of the SSN has/or will be applied to this system? (e.g. masking, truncation, alternative identifier)

N/A

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

N/A

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

A. Taxpayer: The ISRP application includes taxpayer data elements and fields from over 200 paper tax forms (i.e. 1040, 1040A, 1040EZ, 1120) and taxpayer checks for forwarding to downstream IRS systems for processing including the following information: • Name • Address • TIN • Filing Status • Tax Period • Amount of Check • Service Center Stamps • Date/Time of Process • Bank Number • All of the information required on the various IRS tax forms and the information contained on individual business checks and remittances B. Employee: The OPSTATS database contains individual operator performance data which is used for incentive pay determination for the Key Entry Operators including: • User Identification (ID) • Data Entry Keystroke Count • Employee Performance Data C. Audit Trail Information: Standard audit trail information is captured within the ISRP application during employee login including: • User ID • Hostname • Date/Time • Login/Logoff • Success/Failure

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.

Auditing is enabled on all infrastructure components by Quest Agents. Deficiency ISRP end users can add, modify and research taxpayer data. ISRP SOP users can modify taxpayer data entered by EOP users. ISRP is not capturing any events associated with these accesses to taxpayer data which occur during the submission and remittance processes. Taxpayer events have not been identified or generated (AU-2, AU-12). The content of the events are not available (AU-3) and the events are not reviewed (AU-6). ISRP SOP users have elevated privileges within the application (TMS) where they can add and delete ISRP users. These actions are not captured (AU-2) Taxpayer events are collected by the Security Audit and Analysis System (SAAS) for review for inappropriate access. The login ID for ISRP is a three character id and it is linked incentive pay. The Login ID should be the SEID or SSN in order to be accepted by SAAS. In the future, ISRP has a plan to replace the three character code with the SEID. ISRP submitted a signed Risk Acceptance (RA) Form 14201 (signed 04.23.13) to the ESAT PMO on 04.25.13 for the AU-2, AU-3, AU-6 and AU-12 control deficiencies related to access to taxpayer data. ISRP communicated that major engineering analysis and re-engineering of the current ISRP system would be required to develop an automated functionality to send Transcriber Taxpayer Data Entry data directly to SAAS. Currently the Paper Processing Branch (PPB) does not have a Performance Work Request (PWR) to begin the engineering analysis that would lead to re-engineering the ISRP system to accomplish this process. Funding for the PWR would also be required. At the present time the PPB is not in a position to fund a PWR.

11a. Does the audit trail contain the audit trail elements as required in current IRM 10.8.3 *Audit Logging Security Standards*? Yes

12. What are the sources of the PII in the system? Please indicate specific sources:

- a. IRS files and databases: No
If **Yes**, the system(s) are listed below:
No System Records found.
- b. Other federal agency or agencies: No
If **Yes**, please list the agency (or agencies) below:
- c. State and local agency or agencies: No
If **Yes**, please list the agency (or agencies) below:
- d. Third party sources: No
If yes, the third party sources that were used are:
- e. Taxpayers (such as the 1040): No
- f. Employees (such as the I-9): No
- g. Other: No If **Yes**, specify:

C. PURPOSE OF COLLECTION

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

13. What is the business need for the collection of PII in this system? Be specific.

The business purpose of the application is to capture all paper tax information data for further processing by other IRS systems. ISRP supports all IRS tax forms.

D. PII USAGE

Authority: OMB M 03-22 & PVR #16, Acceptable Use

14. What is the specific use(s) of the PII?

- To conduct tax administration Yes
- To provide taxpayer services Yes
- To collect demographic data No
- For employee purposes No

If other, what is the use?

Other: No

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:	_____	<i>If other, specify:</i> _____

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? No

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? No

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

20. Did any of the PII provided to this system originate from any IRS issued forms?

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	_____
Website Opt In or Out option	_____
Published System of Records Notice in the Federal Register	_____
Other:	_____

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:

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>Yes</u>	
Users		<u>Read Only</u>
Managers		<u>Read Only</u>
System Administrators		<u>Read Only</u>
Developers		<u>Read Write</u>
Contractors:	<u>No</u>	

Contractor Users	_____	_____
Contractor System Administrators	_____	_____
Contractor Developers	_____	_____
Other:	No	_____

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?

Contractors do not have access to the data within the application. ISRP has identified the following users and their permissions: Submission Processing = SP Remittance Processing = RP User Permissions/Role SP Data Entry Operator (EOP) • Login privilege restricted to only ISRP data entry workstations. • Windows Explorer access severely restricted (i.e. access to only pertinent data entry applications, no file system access, etc.) • Access to ISRP Data Entry Operations application • Access to IDRS through Info Connect application RP/Transaction Management System (TMS) Data Entry Operators • Login privilege restricted to only ISRP data entry workstations • Windows Explorer access severely restricted (i.e. access to only pertinent data entry applications, no file system access, etc.) • Access to TMS data entry application SP Supervisory Operator (SOP) • Login privilege restricted to only ISRP data entry workstations • Windows Explorer access severely restricted (i.e. access to only pertinent data entry applications, no file system access, etc.) • Access to ISRP Data Entry Operations application and ISRP Supervisory Operations application RP Supervisory Operator (ROP) • Login privilege restricted to only ISRP data entry workstations • Windows Explorer access severely restricted (i.e. access to only pertinent data entry applications, no file system access, etc.) • Access to TMS data entry application and additional TMS workflow management / supervisory features Batch Scheduler Operator • Login privilege restricted to only ISRP data entry workstations • Windows Explorer access severely restricted (i.e. access to only pertinent data entry applications, no file system access, etc.) • Access to TMS data entry application and additional TMS workflow management, monitoring, and supervisory features RP Stager Users • Login privilege restricted to only ISRP data entry workstations • Windows Explorer access severely restricted (i.e. access to only pertinent data entry applications, no file system access, etc.) • Access to only TMS Stager and TMS Block Extract application RP Track Operator (TO) • Login privilege restricted to only ISRP data entry workstations • Windows Explorer access severely restricted (i.e. access to only pertinent data entry applications, no file system access, etc.) • Access to only TMS Pass 1 / Pass 2 applications RP Car Stager Users • Login privilege restricted to only ISRP data entry workstations • Windows Explorer access severely restricted (i.e. access to only pertinent data entry applications, no file system access, etc.) • Access to only TMS CAR Stager application RP Export Stager Users • Login privilege restricted to only ISRP data entry workstations • Windows Explorer access severely restricted (i.e. access to only pertinent data entry applications, no file system access, etc.) • Access to only TMS Export Stager application • Access to remote into Application Servers to run Export Stager process RP ICR Stager Users • Login privilege restricted to only ISRP data entry workstations • Windows Explorer access severely restricted (i.e. access to only pertinent data entry applications, no file system access, etc.) • Access to only TMS Intelligent Character Recognition (ICR) Stager application RP Polling Users • Login privilege restricted to only ISRP data entry workstations • Windows Explorer access severely restricted (i.e. access to only pertinent data entry applications, no file system access, etc.) • Access to only TMS Reporting Stager application RP Image Capture Server Users • Login privilege restricted to only ISRP data entry workstations • Windows Explorer access severely restricted (i.e. access to only pertinent data entry applications, no file system access, etc.) • Access to only Image Capture Server application SP Quality Review (QR) Operator • Login privilege restricted to only ISRP data entry workstations • Windows Explorer access severely restricted (i.e. access to only pertinent data entry applications, no file system access, etc.) • Access to ISRP Data Entry Operations application and ISRP Supervisory Operations application System Administrators • Domain administrators • Access to SP application administration functions TMS System Administrators • Access to TMS application administration functions. IDRS Users Group • Controls access to Info Connect/IDRS for Standard Operating Procedures (SOPs) Database Administrators (DBAs) • Login privilege restricted to ISRP DBA's • Controls access to ISRP Database Administrative functions Access to the data by a user is determined by the individual's position description. Only individuals who have a valid requirement and need-to-know will be granted access to the ISRP application. All users must receive access via On-Line 5081 (OL5081) to have access to the data within the application. Access to the data within the application is restricted. Users are restricted to only those pieces of the application that they need to complete their job functions. A user's access to the data terminates when the user no longer requires access to ISRP. Yes, other IRS systems do provide, receive, and share data with the ISRP application: Financial Management Information System (FMIS): ISRP outputs remittance data to the CDDB including: End of Day and End of Shift information: • Money Amount • Transaction Volume • Taxpayer ID • Taxpayer

Name • Entity Information Generalized Mainframe Framework (GMF): ISRP transmits data to GMF, which includes IMF and BMF files (sending End of Day and End of Shift processing), via EFTU once a day. This data is yielded from tax forms and once validated and formatted within ISRP, is sent to GMF. End of Day and End of Shift information : • Money Amount • Transaction Volume • Taxpayer ID • Taxpayer Name • Entity Information IDRS: ISRP Entry Operators (EOPs) access IDRS using the terminal emulation software Info Connect to perform research and obtain taxpayer information that is needed during tax document processing. • Taxpayer Name • TIN • Taxpayer Address • Taxpayer Zip Code Incentive Pay System (IPS-PAY): ISRP sends operator statistics, including keying speed and SSA files (received from NAP) to IPS-PAY monthly. NAP: ISRP extracts data via Secure FTP share from the NAP application, including IMF and BMF files on a weekly basis including: • Taxpayer Name • TIN • Taxpayer Address • Filing Status • Tax Period • Information from SSA Remittance Transaction Research (RTR): ISRP sends check images and remittance data to the RTR application via EFTU on a daily basis. The IRSP check images that are sent to RTR include the following information: • Taxpayer Name • Amount of Check • Service Center Stamps • Date/Time of Process • Bank Number MITS-17 Enterprise Systems Domain: ISRP has implemented the Quest InTrust Agent on each ISRP server to enable centralized collection of audit log data from all ISRP servers which is collected by the centralized InTrust infrastructure contained within MITS-17. The following ISRP audit trail information is sent to the MITS-17 General Support System (GSS): • User ID • Hostname • Date/Time • Login/Logoff • Success/Failure Yes, all IRS systems listed above have received an approved Security Certification and Privacy Impact Assessment. FMIS: Security Assessment & Authorization (SA&A) Authority to Operate (ATO) received on March 23, 2009, expires on March 23, 2012. PIA received on January 30, 2009, expires on January 30, 2012. GMF: SA&A ATO received on February 18, 2009, expires on February 18, 2012. PIA received on October 16, 2008, expires on October 16, 2011. IDRS: SA&A ATO received on March 10, 2009, expires on March 10, 2012. PIA received on November 6, 2008, expires on November 6, 2011. IPS-PAY: SA&A ATO received on June 17, 2008, expires on June 17, 2011. PIA received on February 1, 2011, expires on February 1, 2014. NAP: SA&A ATO received on February 13, 2009, expires on February 13, 2012. PIA received on March 23, 2010, expires on March 23, 2013. RTR: SA&A ATO received on April 5, 2010, expires on April 5, 2013. PIA received on November 17, 2009, expires on November 17, 2012. MITS-17 GSS Enterprise Systems Domain: SA&A ATO received on September 24, 2010, expires on September 24, 2013. PIA received on February 19, 2010, expires on February 19, 2013.

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

Data from the paper tax information documents is "keyed-in" and "re-keyed" for comparison by the entry operators. Also various system checks validate the data for accuracy, timeliness, and completeness to include zero balance for math fields, city-state-zip code match, and entity file index checks.

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? Yes

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.

ISRP is a matching and extraction system, and is non-recordkeeping. It is designed to capture, format, and forward information related to tax submissions and remittances in electronically readable formats through the Generalized Mainline Framework (GMF) to downstream IRS systems. ISRP is not the official repository for data and documents. GMF is appropriately scheduled under IRM 1.15.35 Records Control Schedule for Tax Administration Systems (Electronic), Item 19 and other recordkeeping systems are scheduled, as appropriate. ISRP is owned and operated by the Wage and Investment (W&I) Business Unit (BU) and is comprised of two main functions which include Submission Processing, and Remittance Processing. Per IRM 3.24 ISRP System, ISRP data is automatically purged after five days when output to downstream IRS systems is complete. This includes reports, and operator statistics.

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.

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

ISRP follows the IRM and eCM Annual Assessment (eCM AA), the eCM-Reauthorization (eCM-r), and the Event Driven Security Controls Assessment (E-D SCA). Required by Treasury, assessments of all FISMA reportable applications every 365 days.

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

Data transmitted between ISRP campuses and satellite offices (i.e., San Antonio, etc.) are all protected through the use of Cylink NRZ-H link Encryptors using (3DES) encryption, which is handled by GSS-1. Therefore, ISRP relies on GSS-1 for the implementation of this portion of the control. ISRP PDS Environment: Northrup Grumman accesses the routers/switches using a Cisco Works NMS through a dedicated 56k leased line established between the ISRP PDS and the IRS' NCFB facility. The 56k leased line is encrypted using Thales DC2000 Encryptors using (3DES) encryption and has the capability of implementing advance encryption standard (AES) thereby further reducing the risk of access by unauthorized parties. ISRP relies on GSS-1 for the implementation of this portion of the control.

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.

ISRP follows the IRM and eCM Annual Assessment (eCM AA), the eCM-Reauthorization (eCM-r), and the Event Driven Security Controls Assessment (E-D SCA). Required by Treasury, assessments of all FISMA reportable applications every 365 days

29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 - *IT Security, Live Data Protection Policy*? Yes

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

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

12/24/2012

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.

<u>SORNS Number</u>	<u>SORNS Name</u>
24.060	CADE Individual Master File (IMF)
20.046	CADE Business Master File (BMF)
36-003	General Personnel And Payroll Records
34.037	IRS Audit Trail and Security Records

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) No
- Provided viable alternatives to the use of PII within the system No
- New privacy measures have been considered/implemented No
- Other: No

32a. If **Yes** to any of the above, please describe:

NA