**Integrated Submission and Remittance Processing (ISRP) – Privacy Impact Assessment**

**PIA Approval Date – May 3, 2011**

**System Overview:**

The Integrated Submission and Remittance Processing (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. 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. In addition, ISRP uses Enterprise File Transfer Utility (EFTU) to transfer remittance data to the Remittance Transaction Research (RTR) system.

**Systems of Records Notice (SORN):**

- IRS 24.030--Customer Account Data Engine Individual Master File
- IRS 24.046--Customer Account Data Engine Business Master File
- IRS 36.003--General Personnel and Payroll Records
- IRS 34.037--IRS Audit Trail and Security Records

**Data in the System**

**1. Describe the information (data elements and fields) available in the system in the following categories:**

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

**2. Describe/identify which data elements are obtained from files, databases, individuals, or any other sources.**

A. IRS:
   - Integrated Data Retrieval System (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

   - National Accounts Profile (NAP) – ISRP extracts data via Secure FTP share from the NAP application, including Individual Master File (IMF) and Business Master File (BMF) files on a weekly basis including:
     - Taxpayer Name
     - TIN
     - Taxpayer Address
     - Filing Status
     - Tax Period
     - Information from Social Security Administration (SSA)

B. Taxpayer – The sources of information in the system are over 200 taxpayer submitted paper tax forms (i.e. 1040, 1040A, 1040EZ, 1120), checks, and remittance related vouchers, which are the manually entered into the ISRP application. This information includes:
   - Name
   - Address
   - TIN
   - All of the information required on the various IRS tax forms and the information contained on individual business checks and remittances

C. Employee – The ISRP application receives the following information directly from IRSP employees including:
   - User ID
   - Data Entry Keystroke Count
   - Employee Performance Data

**3. Is each data item required for the business purpose of the system? Explain.**
Yes. The business purpose of the application is to capture all paper tax information data for further processing by other IRS systems.

**4. How will each data item 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.

**5. Is there another source for the data? Explain how that source is or is not used.**
No. There are no other sources of data.

**6. Generally, how will data be retrieved by the user?**
Taxpayer data is retrieved via ISRP user workstations, which are a part of the ISRP domain. The ISRP domain is a closed network and located in a secure and restricted area at each of the six IRS campuses.

**7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?**
Yes. ISRP data is retrievable from the Document Locator Number (DLN) and TIN.

**Access to the Data**

**8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?**
ISRP has identified the following users and their permissions:

**Role:** Submission Processing Data Entry Operator (EOP)
**Permission:**

- 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 Integrated Data Retrieval System (IDRS) through Info Connect application

**Role:** Remittance Processing /Transaction Management System (TMS) Data Entry Operators
**Privilege:**

- 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

**Role:** Submission Processing Supervisory Operator (SOP)
**Privilege:**

- 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

**Role:** Remittance Processing Supervisory Operator (ROP)
**Privilege:**

- 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

**Role**: Batch Scheduler Operator
**Privilege**:

- 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

**Role:** Remittance Processing Stager Users
**Privilege:**

- 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

**Role:** Remittance Processing Track Operator (TO)
**Privilege:**

- 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

**Role:** Remittance Processing Car Stager Users
**Privilege:**

- 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 Courtesy Amount Read (CAR) Stager application

**Role:** Remittance Processing Export Stager Users
**Privilege:**

- 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

**Role:** Remittance Processing Intelligent Character Recognition (ICR) Stager Users
**Privilege:**

- 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 ICR Stager application

**Role:** Remittance Processing Polling Users
**Privilege:**

- 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

**Role:** Remittance Processing Image Capture Server Users
**Privilege:**
- 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

**Role:** Submission Processing Quality Review (QR) Operator
**Privilege:**
- 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

**Role:** System Administrators
**Privilege:**
- Domain administrators
- Access to SP application administration functions

**Role:** Transaction Management System (TMS) System Administrators
**Privilege:**
- Access to TMS application administration functions.
- IDRS Users Group  Controls access to Info Connect/IDRS for Standard Operating Procedures (SOPs)

**Role:** Database Administrators (DBAs)
**Privilege:**
- Login privilege restricted to ISRP DBA's
- Controls access to ISRP Database Administrative functions

*Note: Contractors do not have access to the application.*

**9. How is access to the data by a user determined and by whom?**
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.

**10. Do other IRS systems provide, receive, or share data in the system? If YES, list the system(s) and describe which data is shared.**
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 Custodial Detail Database (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

- Integrated Data Retrieval System (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.

- National Account Profile (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

- Modernization & Information Technology Services (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

**11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?**
Yes, all IRS systems listed above have received an approved Security Certification and Privacy Impact Assessment.

Financial Management Information System (FMIS)
- Security Assessment & Authorization (SA&A) Authority to Operate (ATO) – March 23, 2009, expires on March 23, 2012.
- Privacy Impact Assessment (PIA) – January 30, 2009, expires on January 30, 2012.

Generalized Mainframe Framework (GMF)
- Security Assessment & Authorization (SA&A) Authority to Operate (ATO) – February 18, 2009, expires on February 18, 2012.
- Privacy Impact Assessment (PIA) – October 16, 2008, expires on October 16, 2011.

Integrated Data Retrieval System (IDRS)
- Security Assessment & Authorization (SA&A) Authority to Operate (ATO) – March 10, 2009, expires on March 10, 2012.
- Privacy Impact Assessment (PIA) – November 6, 2008, expires on November 6, 2011.

Incentive Pay System (IPS–PAY)
- Security Assessment & Authorization (SA&A) Authority to Operate (ATO) – June 17, 2008, expires on June 17, 2011.
- Privacy Impact Assessment (PIA) – February 1, 2011, expires on February 1, 2014.

National Account Profile (NAP)
- Security Assessment & Authorization (SA&A) Authority to Operate (ATO) – February 13, 2009, expires on February 13, 2012.
- Privacy Impact Assessment (PIA) – March 23, 2010, expires on March 23, 2013.

Remittance Transaction Research (RTR)
- Security Assessment & Authorization (SA&A) Authority to Operate (ATO) – April 5, 2010, expires on April 5, 2013.
- Privacy Impact Assessment (PIA) – November 17, 2009, expires on November 17, 2012.

Modernization & Information Technology Services (MITS) –17 General Support System (GSS) Enterprise Systems Domain:
- Security Assessment & Authorization (SA&A) Authority to Operate (ATO) – September 24, 2010, expires on September 24, 2013.
- Privacy Impact Assessment (PIA) – February 19, 2010, expires on February 19, 2013.

**12. Will other agencies provide, receive, or share data in any form with this system?**
No. Other agencies do not provide, receive, or share data with ISRP.

## Administrative Controls of Data

**13. What are the procedures for eliminating the data at the end of the retention period?**
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.

**14. Will this system use technology in a new way?**
No. ISRP is not using technology in new ways that the IRS has not previously employed.

**15. Will this system be used to identify or locate individuals or groups? If so, describe the business purpose for this capability.**
No. The ISRP system is not used to identify or locate individuals or groups.

**16. Will this system provide the capability to monitor individuals or groups? If yes, describe the business purpose for this capability and the controls established to prevent unauthorized monitoring.**
No. The ISRP system is not used to monitor individuals or groups.

**17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?**
No. Use of the system cannot allow IRS to treat taxpayers, employees, or others, differently.

**18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?**
No. The ISRP system does not examine taxpayer data for positive or negative determinations.

**19. If the system is web–based, does it use persistent cookies or other tracking devices to identify web visitors?**
Not applicable. ISRP is not a web–based system.

**View other PIAs on IRS.gov**