Remittance Strategy for Paper Check Conversion (RS–PCC) – Privacy Impact Assessment

PIA Approval Date – Sept. 29, 2010

System Overview:

The Remittance Strategy for Paper Check Conversion (RS–PCC) system allows paper checks (remittances) to be immediately converted to electronic transactions at the time and place of receipt, reducing payment deposit and posting times, and eliminating the need to manually transport most paper checks to Submission Processing Centers (SPC). The RS–PCC system enables the Consolidated Campuses, Taxpayer Assistance Centers (TACs) and Revenue Officers (ROs) to electronically process paper remittances at the point of receipt. Using equipment at these locations, the employee can scan the check and the payment voucher. The equipment captures the image and necessary data on each document. The data is forwarded to the Federal Reserve payment system for immediate deposit. Confirmations are returned, enabling the subsequent accounting actions to occur, including the withdrawal of the check amount and crediting payments to the taxpayer's account.

Systems of Records Notice (SORN):

- IRS 22.054--Subsidiary Accounting Files
- IRS 24.030--CADE Individual Master File (IMF)
- IRS 24.046--CADE Business Master File (BMF)
- IRS 26.019--Taxpayer Delinquent Account (TDA) Files
- IRS 34.037--IRS Audit Trail and Security Records System

Data in the System

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

A. Taxpayer – The following remittance data is collected on the taxpayer:
   - Check Data
   - Check Number
   - Account Number
   - Routing Number
   - Dollar Amount
   - Name
   - Taxpayer Identification Number (TIN)
   - Transaction Date
   - Document Locator Number (DLN)
   - Telephone Number

   Additional information may be included on the check by the taxpayer, but is not specifically requested or required by the system. Typical data elements that may be added to the check are:
   - Address

B. Employee – Data which will be collected on the employee during authentication includes:
   - Standard Employee ID (SEID)
   - Password

C. Audit Trail Information – Data which will be collected on employees in audit trails:
    - SEID
    - Date and time of the event
    - Type of event
    - Outcome status
    - Source of Event (IP Address of the originating Workstation of the auditable event)
    - If there is an associated TIN with the event that will be included as well.

D. Other – Insolvency Checks are occasionally submitted by State attorneys or trustees on behalf of the taxpayer including:
    - Check Amount
    - Name Control
    - Master File Table (MFT)
    - TIN/TYPE (Individual or Business)
    - Social Security Number (SSN)/Employee Identification Number (EIN)
    - Remittance Processing System Identification (RPSID)
    - IRS Received Date
    - Tax Period and Year
    - Designated Payment Code
    - Primary Transaction Code and Amount
    - Secondary Transaction Code and Amount

    Another type of data in the system is the Item Reference Number (IRN) reference number used to coordinate with Electronic Verification and Imaging System (ELVIS) and associated deposit ticket.

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

A. IRS:
    - Electronic Federal Payment Posting System (EFPPS):
        - DLN
        - Trace ID
    - MITS–18 (Enterprise Application Integration Broker (EAIB):
        - Dependant TIN
        - Summary information about taxpayer account

B. Taxpayer:
    - Check Data
    - Check Number
    - Account Number
    - Routing Number
    - Dollar Amount
    - Name
    - Taxpayer Identification Number (TIN)
    - Address
    - Telephone Number

C. Employee:
    - SEID
    - Active Directory Password

D. Other Federal Agencies:
    - Financial Management Service Electronic Verification and Imaging System (FMS–ELVIS):
        - Deposit Ticket Number
        - Deposit Amount

E. Other Third Party Sources – Insolvency Checks are occasionally submitted by State attorneys or trustees on behalf of the taxpayer. This data includes:
    - Check Amount
    - Name Control
    - MFT
    - TIN/TYPE (Individual or Business)
    - SSN/EIN
    - RPSID
    - IRS Received Date
    - Tax Period and Year
    - Designated Payment Code
    - Primary Transaction Code and Amount
    - Secondary Transaction Code and Amount

3. Is each data item required for the business purpose of the system? Explain.
Yes, all data items are required to accurately deposit, apply, or correct payments that are associated with a taxpayer's account.

4. How will each data item be verified for accuracy, timeliness, and completeness?
Financial Management Service Electronic Verification and Imaging System (FMS–ELVIS) returns the ticket number upon the completion of the transaction. This is used to verify that the amount of money that the check was written for is the amount of money deposited. FMS–ELVIS returns a deposit ticket summary, which includes the Item Reference Number (generated at the client) and the amount of the transaction that was deposited the previous day. If the amount doesn't reconcile, it is fixed manually. RS–PCC goes forward with the FMS–ELVIS amount and an Accounting Technician has to submit a debit voucher. The transaction data from the remittance will be verified before it is sent to the server. Some of the data will be populated into the system automatically including: amount, check number, account number and routing number. Additionally, users/persons entering the transaction, for example frontline operators or managers, will manually use IDRS or AIS to verify other data elements in the system. It will not let the transaction move forward if data is not entered for each required field. The system will require the user to enter a value for each required field. The data in the system is considered current because it is provided directly from the taxpayer and is dated.

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?
The scope of the data the user can see is limited based on location of user. Thus, somebody from Andover can't view payments from Memphis. The ability to see data is dependent on role and location. Users don't retrieve data, but data is delivered based on their privilege.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?
Yes, there is a list view of items in a location, which may include TIN. Users have the ability to locate a payment based on TINs or Name Control.

Access to the Data

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?

Role: Entry Operators
Permission: Create new payments, edit or delete those payments that have not been submitted for deposit, print, and view reports.

Role: Supervisors
Permission: Managers will have access to the SEID numbers of employees who fall under their operational control. These managers view the status of payments while the data remains in the system.

Role: Analysts
Permission: Analysts have the ability to view status of payments, while data remains in system.

Role: System Administrators (SA):
Permission: An SA is able to administer user accounts (Online 5081 accounts), apply patches/updates to the platform/ environment under the transmittal process and also work to resolve Information Technology Asset Management System (ITAMS) tickets at the request of the business. While the SA has no direct access to the data, the SA has access to archived transmission files that are used in the event that a transmission to one of the application interfaces fails and requires re-transmission. In this scenario the SA may have potential access to taxpayer information. However, all actions by the SA are recorded in the audit logs; the SA does not have access to these logs. They are sent directly to the Security Audit and Analysis System (SAAS). The SA is also required to certify that he/she has performed unauthorized access (UNAX) training annually.

Role: Database Administrators (DBA)
Permission: DBAs control the SYS and SYSTEM accounts in all Oracle databases and therefore require the ability to access all data in the database. These privileges, which include the ability to rewrite, edit and delete if necessary, are required in order for the DBA to fulfil their managerial roles within the system. There are standard auditing functionalities to record the DBA's session.

9. How is access to the data by a user determined and by whom?
All users requesting access to an IRS system must do so through the Online 5081 (OL5081) process. Users are required to complete an OL5081, Information System User Registration/Change Request form, which lists mandatory rules for users of IRS information and information systems. When a user has been approved for access to the application by his/her manager, the OL5081 system sends an email to the user, providing an approval notification. From the OL5081, the user is added to one of three groups based on role. Access to data is limited to group within Active Directory, and location of the user. Limiting active directory to three groups, and location identifier within active directory to limit the data access further.

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.

- Electronic Federal Payment Posting System (EFPPS) – EFPPS accepts taxpayer data and remittance information, and transmits that information to the Master File. Electronic Federal Tax Payment System (EFTPS) also interfaces with IRACS for accounting and reconciliation purposes. For RS–PCC transactions, EFTPS assigns the document locator number (DLN) and the Trace ID. EFTPS will also interface with IDRS to update the TIF image created by RS–PCC and to journaling information to Interim Revenue Accounting Control System (IRACS). However, they do not have direct access to any of the data in RS–PCC. Data received from EFPPS includes:
  - DLN
  - Trace ID

  RS–PCC sends over a transaction and image of check that includes Taxpayer, Name control.

- MITS–18 (Enterprise Application Integration Broker (EAIB)):
  - Dependant TIN
  - Summary information about taxpayer account
  - Returns TINs in negative TIN list
  - Employee SEID

- Remittance Transaction Research (RTR) – this system is an archive tool that provides historical tax payment information. RTR is also used by the IRS to perform payment research. RTR will store remittance transaction data and images for payments processed through RS–PCC. RTR only receives data from RS–PCC and does not provide data. Remittance information includes:
  - Actual image of check
  - Routing number
  - Tax Codes
  - TIN
  - Name Control
  - Amount of transaction
  - DLN
  - Trace ID

- Security Audit and Analysis System (SAAS) – RS–PCC provides audit trail information to SAAS.
  - SEID
  - Date and time of the event
  - Type of event
  - Type of event
  - Outcome status
  - Source of Event (IP Address of the originating Workstation of the auditable event)
  - If there is an associated TIN with the event that will be included as well.

11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?

Electronic Federal Payment Posting System (EFPPS)

- Certification and Accreditation (C&A) Authority to Operate (ATO) – March 19, 2010, expires on March 19, 2013.

- Privacy Impact Assessment (PIA) – January 5, 2010, expires on January 5, 2013.

MITS−18 (Enterprise Application Integration Broker (EAIB)):
- Certification and Accreditation (C&A) Authority to Operate (ATO) – June 2, 2008, expires on June 2, 2011.
- Privacy Impact Assessment (PIA) – April 29, 2010, expires on April 29, 2013.

Remittance Transaction Research (RTR):
- Certification and Accreditation (C&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.

Security Audit and Analysis System (SAAS):
- Certification and Accreditation (C&A) Authority to Operate (ATO) – June 9, 2010, expires on June 9, 2013.
- Privacy Impact Assessment (PIA) – April 9, 2010, expires on April 9, 2013.

12. Will other agencies provide, receive, or share data in any form with this system?
Financial Management Service Electronic Verification and Imaging System (FMS ELVIS):
The Central Image Research Archive (CIRA) located within the Electronic Verification and Imaging System (ELVIS) is used by the FMS to deposit a remittance in the Federal Reserve Bank (FRB). The FRB has the responsibility to debit the taxpayer account.

The RS–PCC system will send remittance transaction data and images to FMS ELVIS after a payment has been processed. RS–PCC will not transmit taxpayer account information to FMS ELVIS. However, the image of the check may also include the Taxpayer Identification Number (TIN) if the information is printed on the check or the Taxpayer has entered the information on the check. FMS ELVIS provides confirmation of the deposit. FMS ELVIS will not have direct access to any of the data in the system.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?
RS–PCC is unscheduled. A request for records disposition authority for RS–PCC and associated records is currently being drafted with the assistance of the IRS Records and Information Management (RIM) Program Office. When approved by the National Archives and Records Administration (NARA), disposition instructions for RS–PCC inputs, system data, outputs, and system documentation will be published under Internal Revenue Manual (IRM) 1.15.35 Records Control Schedule for Tax Administration Systems, item number to be determined.

Submissions Processing is proposing short-term temporary dispositions for system data and associated records. Every transaction submitted to the server from the workstations will have a timestamp on the record in the database. Data successfully or unsuccessfully transmitted will be automatically purged via a system job from the server at different intervals. The physical checks are to be shredded within 14 business days after they are scanned for processing. The shredder must be located within the unit where the scanned checks are securely stored in locked file cabinets. The data in the system will be destroyed after being transmitted to archives, which is 19 calendar days after transfer to the Remittance Transaction Research (RTR) System.

Upon NARA approval of the RS–PCC disposition authority request, the following instructions will be included in all IRMs (i.e., IRM 3.17.278, IRM 21.1.7.5.6.2) and SOPs (currently, only the SOP for Insolvency Operations) that contain RS–PCC procedures:

“The physical checks should not be shredded before 14 days after they are scanned for processing. In no cases should checks be shredded before they have been transmitted for archival in RTR, even if that is later than the 14 days. The shredder must be located within the unit where the scanned checks are securely stored in locked file cabinets.” These procedures will be added to other IRMs and SOPs as RS–PCC capabilities are utilized by other Business Operations.

14. Will this system use technology in a new way?
No. RS–PCC does not use any technologies which are new to the IRS technology environment.

15. Will this system be used to identify or locate individuals or groups? If so, describe the business purpose for this capability.
Yes. The information within RS–PCC does identify individuals and address information on check does provide the location individuals. However, there is not sufficient information gathered on the taxpayer to monitor the individual. Users are only identified in audit logs by their SEID or IP address, which would need to be matched with other information (not available in the system) in order to identify, locate or monitor them.

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 system will not have the capability to identify, locate, and monitor taxpayers or groups.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?
No. The system does not allow the 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 system is not capable of making any determinations on either taxpayers or employers.

19. If the system is web–based, does it use persistent cookies or other tracking devices to identify web visitors?
No. The system does not use persistent cookies or other tracking devices to identify web visitors.

View other PIAs on IRS.gov