Filing Information Returns Electronically (FIRE) – Privacy Impact Assessment

PIA Approval Date – Oct. 25, 2011

System Overview:
Filing Information Returns Electronically (FIRE) enables IRS to reconcile income tax documents (e.g. income from dividends, interest, etc.) filed by taxpayers against those that were provided via forms such as 1099–DIV. FIRE receives incoming electronic files from external trading partners and passes the files or information to the Automated Magnetic Media Processing System (AMMPS), Chapter 3 Withholdings (CTW), Automated Tips (AMT), Automated Extensions (AWAX–EAWPMF) or Form 8955 Social Security Administration (SSA), which are located at ECC–MTB. FIRE then receives statistical information back from these downstream programs and posts the data to a SQL database. Under section 6011(e)(2)(A) of the Internal Revenue Code (IRC), any person, including a corporation, partnership, individual, estate, or trust, who is required to file 250 or more information returns must file such returns magnetically or electronically. Note: As of January 1, 2009, Magnetic Media is no longer accepted.

Systems of Records Notice (SORN):
- IRS 22.026--Form 1042–S Index by Name of Recipient
- IRS 22.061--Wage and Information Returns Processing
- IRS 42.021--Compliance Programs and Projects Files
- IRS 34.037--IRS Audit Trails & 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 – Data elements include the following:
- Payer Name
- Payer Address
- Payer Name Control
- Payer Shipping Address
- Payer City
- Payer State
- Payer ZIP Code
- Payers Phone Number
- TCC
- TIN
- Email address

These data elements are contained on the following forms (includes associated form schedules where applicable):
- Form 1042–S, Foreign Person's U.S. Source Income Subject to Withholding
- Form 1097–BTC, Bond Tax Credit
- Form 1098, including all associated schedules
- Form 1099, including all associated schedules
- Form 3921, Exercise of an Incentive Stock Option Under Section 422(b)
- Form 3922, Transfer of Stock Acquired Through an Employee Stock Purchase Plan Under Section 423(c)

- Form 5498, IRA Contribution Information, including all associated schedules
- Form W–2G, Certain Gambling Winnings
- Form 8027, Employer's Annual Information Return of Tip Income and Allocated Tips
- Form 8809, Extension of Time to File Requests.
- Form 8935, Airline Payments Report
- Form 8955–SSA, Annual Registration Statement Identifying Separated Participants with Deferred Vested Benefits.

B. Employee – Data used in this system consists of Identification and Authentication (I&A) data of FIRE users with access to the system. This information includes user ID and password.

C. Audit Trail Information – The following actions on the FIRE web site taken by business trading partners and Customer Service Representatives (CSR) users are recorded in the FIRE audit log:
   - Logon to System
   - Logoff System
   - Change of Password
   - PIN updated
   - New PIN created
   - File uploaded
   - Account created
   - Password reset
   - Updated account information
   - Problem uploading (filename)

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

A. IRS – FIRE receives incoming electronic files from external trading partners and passes the files or information to the:
   - Automated Magnetic Media Processing System (AMMPS)
   - Chapter 3 Withholdings (CTW)
   - Automated TIPS (AMT) and
   - Corporate Research, Research and Support Section

   All are located at ECC–MTB. FIRE then receives statistics back from these downstream programs.

   The type of data sent and received is statistical data (e.g. files successfully or unsuccessfully uploaded by trading partners), updated trading partner information (e.g. address), and updated TCCs.

B. Taxpayer – No information is collected directly from individual taxpayers. However, individual tax data is collected and submitted by the Business Trading Partners.

C. Employee – Beyond user ID and password for login purposes, no information is collected directly from employees.

D. Other Federal Agencies – Federal agencies file information returns as Business Trading Partners. No other data is provided by Federal agencies. The federal agencies included would be those that issue information returns such as for student loans, etc.

E. State and Local Agencies – State and Local Agencies file information returns as Business Trading Partners. No other data is provided by State or Local Agencies.

F. Other Third Party Sources – The FIRE system receives information from trading partners. The trading partners can only transmit data files and check on the status of the transmissions.

3. Is each data item required for the business purpose of the system? Explain.
Yes. All data is required for the business purpose of the system to enable the IRS to reconcile income tax numbers (e.g. income from dividends, interest, etc.) filed by taxpayers against that which was provided to them in the form of a form such as 1099–DIV.

4. How will each data item be verified for accuracy, timeliness, and completeness?
It is the responsibility of the business trading partner who sends the data (from their workstation to FIRE) to ensure it is correct, timely and complete, but the payer is responsible for the accuracy of the return and is liable for any penalties. As FIRE makes no changes to data, the data will be as accurate, relevant, timely, and complete as it was when the business trading partner sent it to FIRE. An email is automatically generated and sent within one to two business days (verification) to the business trading partner. In addition, the user can log on the same day the file was sent to verify whether its files have been received by FIRE. The status of the file can be checked one to two business days after submission. Should there be an error in transmission and there is no action by the business trading partner within 21 days of the failed transmission, an email is generated and sent. It is sent every 21 days (starting in April) until the end of the year, or resolution (whichever occurs first).

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

6. Generally, how will data be retrieved by the user?
Business trading partners are required to authenticate to FIRE with their username and password to access the application. Additionally, when a trading partner attempts to submit a file, they must enter their PIN number and have a valid transmitter control code and TIN combination to complete the transmission. The trading partners can only transmit data files and check on the status of their transmissions. Within the application, the trading partner makes a selection (clicks on a button) to obtain data. CSR's are not required to provide a username and password to authenticate to FIRE. The CSR personnel's Standard Employee Identifier (SEID) is passed to FIRE from their Local Area Network (LAN) domain authentication and is checked by the FIRE database for authorization. If the user is a valid FIRE CSR they are granted access, if not, access is denied. CSR's also select buttons within the application to access data.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?
Yes. Records may be retrievable by any of the fields listed below:

- Payer Name
- Payer Address
- Payer Name Control
- Payer Shipping Address
- Payer City
- Payer State
- Payer ZIP Code
- Payers Phone Number

- Transmitter control code (TCC)
- Taxpayer Identification Number (TIN)
- Email address

Access to the Data

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?
Users, System Administrators, and Developers will all have access to data that is relevant and consistent with their designated roles. Access is allowed by On–Line 5081 (OL5081) approval for CSR users and Trading Partner access approval for Trading Partners.

Role: Customer Service Reps
Permission: Users authorized to assist the Trading Partners in researching file submission status and errors.

Role: Trading Partners
Permission: Users authorized to transmit tax return data files and check on the status of the transmissions.

Role: System Administrators
Permission: Users have administrator–level access to the servers that host the FIRE application for the purposes of system administration

Role: Developers
Permission: Users may be granted read–only access to the FIRE application, in accordance with IRS fire call procedures.

Note: Contractors do not have access to the application.

9. How is access to the data by a user determined and by whom?
Business trading partners must submit Form 4419 Application for Information Returns, to request a transmitter control code. Business trading partners mail or fax the form to the Quality Control section for approval. Once the trading partner receives confirmation of account approval they set up their own user ID and password. There is no standard naming convention used for trading partner user IDs.

Data input to FIRE is restricted to the business trading partner submissions of their clients' tax forms. Each business trading partner must be a registered FIRE application user, and must have a valid Transmitter Control Code (TCC) and Taxpayer Identification Number (TIN) combination to successfully submit data to FIRE. If a business trading partner attempts to submit data to the IRS with a non–matching TCC and TIN; FIRE will deny the submission.

Users in the CSR group have their permissions defined via the OL 5081 process. Based on their SEID, they have one of four levels of access in FIRE. All CSR users with access to FIRE must first be approved via the OL 5081 process. Once approved, there is a separate location on the form where access can be requested for FIRE. If this is approved, and the user has been given access to the server where FIRE resides, then access will also be granted within the FIRE application for the rights requested (IT Specialist, Special Projects, Intermediate, or General).

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, FIRE receives incoming electronic files from external trading partners and passes the files or information to the Automated Magnetic Media Processing System (AMMPS), Chapter 3 Withholdings (CTW), Automated TIPS (AMT) and Corporate Research, Research and Support Section, which are located at ECC–MTB. FIRE then receives statistics back from these downstream programs. The statistical information informs FIRE of the transmission status.

The AMMPS and Corporate Research, Research and Support Section programs reside on the IBM mainframe, Modernization & Information Technology Services – 21 General Support Services (MITS–21 GSS). The CTW program resides on the Unisys Mainframe, MITS–23 GSS.

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

IBM Master File Platform (Modernization & Information Technology Services – 21):
- Authorization to Operate (ATO) – February 18, 2010
- Privacy Impact Assessment (PIA) – August 1, 2011

UNISYS Platform (Modernization & Information Technology Services – 23):
- Authorization to Operate (ATO) – September 27, 2010
- Privacy Impact Assessment (PIA) – November 23, 2009

12. Will other agencies provide, receive, or share data in any form with this system?
Yes, various Federal, State and Local Agencies will file information returns as Business Trading Partners. The trading partners can only transmit data files and check on the status of their transmissions.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?
A request for records disposition authority for FIRE 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 FIRE inputs, system data, outputs and system documentation will be published in IRM 1.15.29, Records Control Schedule for Submissions Processing Campus Records, item number to be determined. Current business practice dictates that FIRE data be archived to the Storage Area Network (SAN). The business unit has proposed a data retention of at least three years, but not longer than four years.

14. Will this system use technology in a new way?
No, this system does not use technology in a new way.

15. Will this system be used to identify or locate individuals or groups? If so, describe the business purpose for this capability.
Yes, this system is used to identify any trading partners that pose as fraudulent entities.

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.

Yes, this system is used to monitor individuals for the purpose of identifying any trading partners that pose as fraudulent entities. Unauthorized monitoring is controlled by user access controls.

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

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?
Due process is not applicable. The purpose of FIRE is not to capture data about individuals or make negative determinations about individuals, companies, or their tax related matters. System management is responsible for the proper operation of the system, ensuring correct processing and responses to Business Trading Partners, as well as the oversight of employee use of the system and the data contained therein. If any individuals are identified as fraudulent entities, their information is sent to Criminal Investigation for further action.

19. If the system is web–based, does it use persistent cookies or other tracking devices to identify web visitors?
Yes, the system is web–based, but persistent cookies are not used. The FIRE web site requires session cookies to be accepted by the user's browser. An encrypted cookie is stored on the user's browser that stores the username. No other information is cached or stored in the user's browser or workstation. Session cookies are terminated when the user exits from the web browser session.

View other PIAs on IRS.gov