Electronic Fraud Detection System (EFDS) – Privacy Impact Assessment

PIA Approval Date – Dec. 17, 2010

System Overview:

The Electronic Fraud Detection System (EFDS) is a mission critical, stand–alone automated system designed to maximize fraud detection at the time tax returns are filed to eliminate the issuance of questionable refunds. The EFDS detects reliable indicators of taxpayer fraud, keying highly focused investigations prior to the issuance of the refund, which has resulted in millions of dollars saved by stopping the issuance of fraudulent and erroneous refunds. The EFDS was last used to support live operations for Processing Year (PY) 2010. The EFDS receives data from a variety of sources, including the Third Party Data Store (TPDS), Individual Master File (IMF) including extracts from General Mainline Framework (GMF), Business Master File (BMF), Information Returns Master File (IRMF), Questionable Refund Program (QRP), Modernized e–File (MeF), Customer Account Data Engine (CADE), Electronic Filing System (ELF).

Systems of Records Notice (SORN):

- IRS 22.061--Individual Return Master File
- IRS 24.030--CADE Individual Master File
- IRS 24.046--CADE Business Master File
- IRS 34.037--IRS Audit Trail and Security Records System
- IRS 42.021--Compliance Programs and Project Files
- IRS 46.002--Criminal Investigation Management Information System
- IRS 46.009--Centralized Evaluation and Processing of Information Items (CEPIIs), Evaluation and Processing of Information (EOI)
- IRS 46.050--Automated Information Analysis System

Data in the System

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

A. Taxpayer: Taxpayer information includes most of the tax returns filed for the current year and the 3 previous years, all taxpayer information submitted via electronic or paper, as well as information provided for application for electronic filing is included in the system. This information includes:
   - Taxpayer name
   - Taxpayer Identification Number (TIN)
   - Address
   - Telephone number
   - Social Security number (SSN)
   - Income information
   - Document Locator Number (DLN)
   - Type of return filed (e.g., 1040, 1040A, 1040EZ)
   - Source of filing (paper or electronic)
   - Tax filing status
   - Number of dependents
   - Employer name

- Federal Employer Identification Number (FEIN)
- Employer address

B. Employee
    - Name
    - EFDS User ID
    - Telephone number
    - Fax number
    - Badge number
    - Operating system password (encrypted)
    - Application password (encrypted)
    - Scheme Development Center (SDC)

C. Audit Trail Information: Auditing is mainly performed through the use of database triggers. Triggers are Structured Query Language (SQL) procedures that are implicitly executed when an Insert, Update, or Delete statement is issued against a database table. The data fields and audit functions collected by the system include:
    - EFDS User login ID
    - Group ID
    - Service Center Code
    - Workstation ID
    - Program ID
    - Record ID
    - Table ID
    - System date
    - Action date
    - Run date
    - View date
    - Tax Examiner (TE) code
    - Query type
    - Record type
    - Action type
    - Event
    - Field name
    - Number of rows retrieved
    - DLN
    - Employer Identification Number (EIN)
    - Table changed

D. Other
    - Federal/State Bureau of Prisons:
        - Business Establishment Information:
        - Electronic Filing Identification Number (EFIN) employer identification number
        - Telephone number
        - Address listing
        - Personal information of incarcerated prisoner:
        - Prisoner name
        - Date of birth
        - SSN

- Inmate number
- Incarceration date
- Work release date
- Fugitive code
- Prison code
- Institution name
- Address list of prisons
- Prison institution record:
- Prison code, internal
- Institution name
- Address
- Contact title
- Prison phone number
- Commercial public business telephone

- Department of Health and Human Services (HHS):
  - Employee name
  - Employee address
  - SSN
  - Employer name
  - FEIN
  - Employer address
  - Wage amount

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

A. IRS

- Third Party Data Store (TPDS) – List of applicants for electronic filing, firm name, addresses, EFIN, contact persons, phone numbers, type of filer, electronic transmitter identification number (ETIN).
- Business Master File (BMF) – Master list of employers/payers and data extracted from the Business Return Transaction File (BRTF).
- Individual Master File (IMF) – Tax return information filed by individuals for the previous 3 years.
- Information Returns Master File (IRMF) – Information documents, W–2s, Form 1099s (U.S. Information Return for Calendar Year X).
- Questionable Refund Program (QRP) – Data elements passed through the pipeline processing stream that historically have been found useful in determining if the return contains fraudulent information.
- Electronic Filing System (ELF) – Data elements passed through the pipeline processing stream that historically have been found useful in determining if the return contains fraudulent information.
- Generalized Mainline Framework (GMF) – Electronically filed (e–filed) Form 1040 series individual income tax returns. Data elements passed through the pipeline processing stream that historically have been found useful in determining if the return contains fraudulent information.
- Modernized e–File (MeF) – Data elements passed through the pipeline processing stream that historically have been found useful in determining if the return contains fraudulent information.

Taxpayer and employer/payer information is submitted to the IRS via electronic and paper formats. Most of the current year taxpayer information, plus the 3 previous years' information, is in EFDS.

B. Taxpayer: Taxpayer name, address, telephone number, SSN, and completed line items on the tax return and any attached schedules as filed by the taxpayer or his representative. This refers to anything in an electronically/paper filed return (with the exception of paper returns which are "balance due" and all balanced returns where the taxpayer has claimed earned income tax credit).

C. Employee: Employee first and last name, User ID, IRS Campus location, phone number, fax number, badge number (employee ID), roles, user status, operating system password, application password and access privilege levels and district office assignments.

D. Other Federal Agencies:
   - Federal/State Bureau of Prisons delivers prisoner listing information annually to CI in electronic format. From this information the data is converted and a file is built and loaded into EFDS. See Question 1 for list of data elements.

   - HHS provides a data matching service for matching EFDS data with the National Directory of New Hires (NDNH) database. This cross matching validates wage and employment information for all verified SSNs provided.

E. State and Local Agencies: All states and the District of Columbia prisons deliver prisoner listing information annually to CI in electronic format. See Question 1 for list of data elements.

F. Other Third Party Sources: Commercial public business telephone directory listings/databases are purchased by CI to contact employers for employment and wage information. CI updates this database manually with correct information.

3. Is each data item required for the business purpose of the system? Explain.
Yes. EFDS is a mission critical, automated system designed to maximize fraud detection at the time that tax returns are filed to reduce the issuing of questionable refunds. All data items compiled by the EFDS are used to cross–reference and verify information that relates to potentially fraudulent tax returns. Each data element present is necessary to support the business purpose of the system.

4. How will each data item be verified for accuracy, timeliness, and completeness?
Due to the nature of the EFDS application, all input data is accepted as received. The application does not have the capability to modify the data that is received. This is outside of the EFDS scope.

5. Is there another source for the data? Explain how that source is or is not used.
No. Data is not collected from another source beyond what has been stated previously in Question 2.

6. Generally, how will data be retrieved by the user?
EFDS users submit queries to retrieve data from the system. Any data element in the system is a query field.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?
Yes. Data is retrievable by a personal or unique identifier (e.g., SSN, name) or any of the data elements mentioned in Question 1, Section A.

Access to the Data

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?
EFDS has approximately 600 authorized CI, W&I and SB/SE personnel that use the application for the investigation of potential fraudulent tax refunds. The users of EFDS are:

Role: System Users (Investigative Aides/Analysts)
Permission: Perform queries, update records with wage verification information, and update employer contact information.

Role: System Administrator
Permission: Assigns user roles, gives permissions and oversees access to the system, manages system backup and maintain the EFDS database, and protects access IDs and codes from any misuse and improper disclosure. Installs database and loads transmittals.

Role: Database Administrator
Permission: Performs database maintenance functions and troubleshooting.

Role: First Line Managers
Permission: Verify that EFDS users have appropriate clearances, authorizations, need–to–know, and security training prior to being given access to the system.

Role: System Security Administrator
Permission: Ensures that contractors involved in the development, operation, or maintenance of the EFDS have appropriate clearances, authorizations, need–to–know, and security training on safeguards and implementation procedures at least every three years. Oversees any security breach issues and acts to confirm through the Online 5081 system that users have the proper background clearances. Tracks all security issues related to users.

Role: Criminal Investigation Program Analysts
Permission: Oversight functions and program management

Role: Data Storage Administrator
Permission: Manages the storage of EFDS data.

Role: SB/SE Tax Examiners
Permission: Perform queries, but only have read–only access. Cannot update or make changes.

Role: W&I Tax Examiners
Permission: Perform queries, update records with wage verification information, update employer contact information, and screen and review returns to detect questionable returns.

Note: Currently, no contractors hold any of the EFDS user roles.

9. How is access to the data by a user determined and by whom?
All access credential requests are enforced through the Online 5081 process for granting permissions to systems and applications used by IRS personnel. Employees must complete and submit an Online 5081 request for EFDS access. The form contains information on the permissions or role to be assigned to the account. The request is forwarded to the employee's manager (or Functional Security Coordinator) and the system administrator of the application for approval. The manager and system administrator review the Online 5081 request to ensure that the correct access privileges listed on the form correspond to the user's job requirements. If everything is accurate, both the manager and system administrator must electronically sign off on the form. As a final step, the requesting user must also sign off agreeing that access to the application is required. A user's access to the data terminates when it is no longer required.

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. EFDS receives data from files listed below:

- Third Party Data Store (TPDS) – List of applicants for electronic filing, firm name, addresses, EFIN, contact persons, phone numbers, type of filer, electronic transmitter identification number (ETIN).
- Business Master File (BMF) – Master list of employers/payers and data extracted from the Business Return Transaction File (BRTF).
- Individual Master File (IMF) – Tax return information filed by individuals for the previous 3 years.
- Information Returns Master File (IRMF) – Information documents, W–2s, Form 1099s (U.S. Information Return for Calendar Year X).
- Questionable Refund Program (QRP) – Data elements passed through the pipeline processing stream that historically have been found useful in determining if the return contains fraudulent information.
- Electronic Filing System (ELF) – Data elements passed through the pipeline processing stream that historically have been found useful in determining if the return contains fraudulent information.
- Generalized Mainline Framework (GMF) – Electronically filed (e–filed) Form 1040 series individual income tax returns. Data elements passed through the pipeline processing stream that historically have been found useful in determining if the return contains fraudulent information.
- Modernized e–File (MeF) – Data elements passed through the pipeline processing stream that historically have been found useful in determining if the return contains fraudulent information.
- Customer Accounting Data Engine (CADE) receives a transaction code to remove a taxpayer account from the CADE application.

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

Third Party Data Store (TPDS) is a subset of E–Services

- Certification & Accreditation (C&A) – April 2, 2008
- Privacy Impact Assessment (PIA) – November 26, 2007

Business Master File (BMF)

- Certification & Accreditation (C&A) – June 14, 2010
- Privacy Impact Assessment (PIA) – March 16, 2010

Individual Master File (IMF)
- Certification & Accreditation (C&A) – March 8, 2010
- Privacy Impact Assessment (PIA) – November 10, 2009

Information Returns Master File (IRMF) is a subsystem of Information Returns Processing (IRP)
- Certification & Accreditation (C&A) – March 8, 2010
- Privacy Impact Assessment (PIA) – October 9, 2009

Customer Accounting Data Engine (CADE)
- Certification & Accreditation (C&A) – April 2, 2009
- Privacy Impact Assessment (PIA) – October 19, 2009

Electronic Filing System (ELF)
- Certification & Accreditation (C&A) – May 26, 2009
- Privacy Impact Assessment (PIA) – April 15, 2009

Generalized Mainline Framework (GMF)
- Certification & Accreditation (C&A) – February 18, 2009
- Privacy Impact Assessment (PIA) – October 16, 2008

Questionable Refund Program (QRP) is a subsystem of EFDS
- Certification & Accreditation (C&A) – June 20, 2008
- Privacy Impact Assessment (PIA) – October 7, 2008

Modernized e–File (MeF)
- Certification & Accreditation (C&A) – May 14, 2010
- Privacy Impact Assessment (PIA) – October 23, 2009

12. Will other agencies provide, receive, or share data in any form with this system?
Yes. EFDS receives data from HHS, the Federal Bureau of Prisons and state prisons.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?
Records are maintained, administered and disposed of in accordance per Internal Revenue Manual (IRM) 1.15.30, Records Management, Records Control Schedule for Criminal Investigation, January 1, 2003, Item number 15, Investigative Files. Audit logs are maintained in compliance to IRM 10.8.3, Audit Logging Security Standards.

14. Will this system use technology in a new way?
No. This system will 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. The purpose of the system is to identify individuals or groups committing fraud in filing, either electronically or paper filed individual returns. The purpose is to protect IRS revenue streams by detecting current fraudulent activity and preventing future recurrences.

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 and groups who have filed suspected fraudulent returns. The purpose is to protect IRS revenue streams by detecting current fraudulent activity and preventing future recurrences. The system is on a closed, sensitive but unclassified network via a secure local area network (LAN). All workstations are secured and the only way to access the application is to obtain a user account via the Online 5081 process. Additionally, all user activities are audited.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?
No. Once fraud is suspected, laws and administrative procedures, policies and controls govern the ensuing actions.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?
No. EFDS does not make any negative determinations. Once fraud is suspected, laws and administrative procedures, policies, and controls govern criminal investigations or any other the ensuing actions. Due process is awarded during any ensuing criminal investigation or civil action.

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

View other PIAs on IRS.gov