Criminal Investigation (CI) Electronic Fraud Detection System (EFDS)
Privacy Impact Assessment

PIA Approval Date – Oct. 30, 2006

System Overview

The Electronic Fraud Detection System (EFDS) is a compliance system within the Enforcement Division, Compliance Domain that provides tools needed to perform pre-refund detection of potentially criminal fraudulent tax returns and civil fraud Earned Income Tax Credit (EITC) and other Examination issues. It is currently used primarily to examine electronically filed returns, but also provides limited support for all return filing modes.

Data in the System

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

The EFDS contains most of the current tax year individual filed tax returns. A comparison of on-line prior year data, including W-2 information, with the current tax return allows the Criminal Investigation (CI) Investigative Aides/Analysts (IA/As) to make better decisions on cases where federal tax returns are identified as potentially fraudulent.

    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
- 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

    B. Employee:
- name
- USERID
- IRS Campus location
- telephone number
- fax number
- badge number

    C. Audit Trail: Auditing is mainly performed through the use of database triggers. Triggers are 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:
- user login ID
- group ID
- SC code
- workstation ID
- program ID
- record ID

- table ID
- system date,
- action date
- run date
- view date
- TE (tax examiner) code
- query type
- record type
- action type
- event
- field name
- # of rows retrieved
- DLN
- EIN
- table changed

D. Other:
- 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
  -social security number
  -inmate number
  -incarceration date
  -work release date
  -institution code
  -institution name
- Prison institution record:
  -institution code
  -institution name
  -address
  -contact title
  -prison phone number
  -commercial public business

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, W2s (Wage and Tax Statement), 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.

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: The source is the electronically/paper filed return. Taxpayer name, address, telephone number, social security number, and all 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.

C. Employee: Source of employee information is the Online 5081. Employee first and last name, USERID, IRS Campus location, phone number, fax number, badge number (employee ID), roles, user status.

D. Other federal agencies:
Federal 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.

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?
All input data is accepted as received.

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 Item 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 1A.

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 personnel that use the application for the investigation of potential fraudulent tax refunds. The users of EFDS are:

- **System User (Investigative Aide/Analyst (IA)** – Perform queries, update records with wage verification information, update employer contact information.
- **System Administrator** -- Assign user roles/gives permissions and oversee access to the system, manage system backup and maintain the EFDS database, and protect access IDs and codes from any misuse and improper disclosure. Installs database and loads transmittals.
- **Database Administrator** – Perform database maintenance functions and troubleshooting.
- **Managers -**- Verify that EFDS users have appropriate clearances, authorizations, need-to-know, and security training prior to being given access to the system.
- **System Security Specialist** - Ensure 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 Online 5081 that users have the proper background clearances and tracks all security issues related to users.
- **Computer Operations Analyst** -- Responsible for installing workstation transmittals, reporting application problems, and basic troubleshooting.
- **Criminal Investigation Program Analysts** --Oversight functions and program management.

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. CI 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 reviewed by the employee's manager and the EFDS System Security Specialist. 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?
Yes. EFDS receives data from files listed in Question 2A.

11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?
Third Party Data Store is a subset of E-Services
- PIA- 8-15-05
- C&A- 2-24-06

Business Master File
- PIA- 8/22/2003 (expired), *expired* on 8/22/2006
- C&A- 8/16/2004, expires on 8/16/2007

Individual Master File
- PIA- 9/1/2003 (expired), expired on 9/1/2006
- C&A- 8/13/2004, expires on 8/13/2007

Information Returns Master File
- PIA- no previous PIA
- C&A 8/15/2004, expires on 8/15/2007

Questionable Refund Program
- PIA- no previous PIA
  C&A- 1/15/2006, expires on 1/15/2009

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

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 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. It is used to monitor individuals and groups who have filed suspected fraudulent returns.

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](#)