e–trak Voluntary Disclosure Program (e–trak VDP) – Privacy Impact Assessment

PIA Approval Date – Dec. 29, 2011

System Overview

The electronic Voluntary Disclosure Program will provide the Large Mid Size Business organization with the flexibility it requires to store, retrieve, update, and track taxpayer data relative to Voluntary Disclosure information of international offshore transactions. Upon account establishment, cases will be assigned to Revenue Officers, Agents, and Examiners in the field to follow–up with taxpayers to obtain background and financial data concerning a taxpayer's offshore transactions with the emphasis on detecting unreported income.

System of Records Notice (SORN):

- IRS 42.021--Compliance Programs and Project Files
- IRS 42.001--Exam Administrative File
- IRS 42.017--International Enforcement Program Files
- IRS 34.037--IRS Audit Trail and Security Records System
- IRS 42.031--Anti–Money Laundering /Bank Secrecy Act (BSA) and Form

Data in the System

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

A. Taxpayer:
- Name (First, MI, Last)
- Taxpayer Identification Number (TIN) – Social Security Number (SSN)/ Employer Identification Number (EIN)
- Date of Birth (DOB)
- Address, City, State, Zip
- Country
- Phone Number
- Fax
- Taxpayer Power of Attorney (POA Name, Centralized Authorization File (CAF) Number, Type, Firm Name, Address, City, State, Zip, Country, Phone)
- Bank Promoter (Name, Address, City, State, Zip, Country, Phone)
- Bank Professionals (Name, Address, City, State, Zip, Country, Phone)
- Source Funds (Type, Name, EIN, Address, City, State, Zip, Country, Relationship to TP)
- Taxpayer Foreign Accounts (Institution Name, Type, Address, City, State, Zip, Country, Phone, Account Type, Names on Account, Advisor Name, Entity Type, Account Opened How, Date Account Open/Closed, Money Went Where, Money/Financial Institution Money Moved To, Account Balances for Tax Years 2002–2008)
- Taxpayer Foreign Entities (Entity Name, Type, Address, City, State, Zip, Country, Relationship to Taxpayer)
- Assets (Non–cash dollar values for Tax Years 2002–2008)
- Taxpayer Return Adjustment values for Tax Years 2002–2008

B. Employee – Data is entered into e–trak VDP Module by a member of the VDP Office. The system is password protected, and is only seen by personnel on a need to know basis.

- Employee/Analysts name – first, middle, last

- Employee SEID
- Date – assigned to case

C. Audit Trail Information:
- Audit Type
- Time
- Account Name
- Data Object
- Table Name
- Tracking Identification (ID)
- Message
- The audit trail assures that those who use e–VDP Module only have permission to view and use the modules their role allows. The System Administrator (SA) prepares and reviews monitoring reports based on Identity Theft Incident Management (ITIM) established timeframes.

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

A. IRS – Tax history data. Upon account establishment, cases will be assigned to Revenue Officers, Agents, and Examiners in the field to follow–up with taxpayers to obtain background and financial data concerning a taxpayer's offshore transactions with the emphasis on detecting unreported income. The following data elements are input into e–trak VDP:
- Tax Year
- Return Type
- Original Adjusted Gross Income (AGI)
- Amended AGI
- AGI Change Amount
- Original Taxable Income
- Amended Taxable Income
- Taxable Income (TI) Change Amount
- Original Tax
- Amended Tax
- Tax Change Amount

B. Taxpayer – Discloses their offshore account information when they mail in their Voluntary Disclosure package to the LB&I International Compliance, Philadelphia Unit. The data elements include:
- SSN/EIN
- DOB
- Last Name
- First Name
- Middle Initial
- Address
- Phone Number
- City
- State
- Zip
- Country

3. Is each data item required for the business purpose of the system? Explain.
Yes, each data item is required for the business purpose of the system. All data collected is required for administering the collection of unreported income from offshore taxpayer income as mandated by the IRS. The data that is collected will be information that facilitates the identification of financial information to determine tax owed.

4. How will each data item be verified for accuracy, timeliness, and completeness?
The e–trak VDP Module identifies and enforces which fields are required to be completed before a record can be saved. Data validation checks are automated in the system to ensure date fields are valid entries and numeric fields are in the valid format. In addition, the Application Administrator prepares and reviews monitoring reports based on Identify Theft Incident Management (ITIM) established timeframes that managers use to validate/verify data.

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

6. Generally, how will data be retrieved by the user?
Users access the e–trak VDP Module using LDAP (Lightweight Directory Access Protocol) authentication. Only authorized users can access e–trak VDP Module and users can only retrieve or handle data based on their assigned user roles. Users access the e–trak VDP Module by authenticating at a login screen using their unique User ID and Password. Users must enter accurate credentials before access is granted to the system.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?
Yes. After logging into the e–trak VDP Module, users are able to access records from the following fields:
- Taxpayer Name (First, MI, Last)
- Taxpayer Identification Number (TIN)
- Examiner
- Power of Attorney
- Bank Promoter
- Bank Professionals
- Source Funds
- Taxpayer Foreign Accounts
- Account Balances
- Taxpayer Foreign Entities
- Offshore Voluntary Disclosure
- Assets
- Taxpayer Return Adjustment values for Tax Years 2002–2008

Access to the Data

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?
The primary users of e–VDP Module include IRS Examiners, Business Owner, Case Builder and Application Administrator. This application does not allow access by the public. Only authorized users are granted authorization to e–trak VDP Module through the On–Line 5081 process.

Role: System Administrator
Privileges: view records, execute SQL queries, view audit data, add users, assigning permissions, review list of accounts

Role: Administrator
Privileges: Administer System Database Administrator (DBA) Access

Role: Examiner
Privileges: Generate User Reports, Create, Add, Edit, Delete, View and Process Cases, Search Cases

Role: VDP Business Owner
Privileges: Generate User Reports, Create, Add, Edit, Delete, View and Process Cases, Search Cases

Role: Case Builder
Privileges: Generate User Reports, Create, Add, Edit, View and Process Cases, Search Cases

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 e–trak VDP Module is determined by submitting an On–Line 5081 and receiving authorization from the user's approval manager. The VDP module is configured for a role–based user access policy. User access is restricted to only the specific application components needed to complete their job function. Logical access controls have been incorporated into VDP for each user; to include assigning access privileges, session controls, and re–certification of users. The users are assigned specific components that they can access as well as the level of access within the module. System Administrators (SAs) are responsible for assigning permissions ensure that the proper permissions are granted to the proper users. All policy and procedures are followed in granting user permissions, determining permissions; ensuring user rights are restricted to the minimum necessary to perform the job, background screening and separation of duties.

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.
No other IRS systems provide, receive, or share data in the system.

11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?
Not Applicable.

12. Will other agencies provide, receive, or share data in any form with this system?
No other agencies provide, receive, or share data in any form with this system.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?
e–trak Voluntary Disclosure Program is unscheduled. A request for records disposition authority for VDP system data 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 e–TRAK VDP inputs,

system data, outputs and system documentation will be published in IRM 1.15, exact Records Control Schedule and item number to be determined.

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.
No, this system will not be 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, this system will not provide the capability to monitor individuals or groups.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?
No, use of this system will not 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 e–trak VDP module does not have the capability to make any negative determinations.

19. If the system is web–based, does it use persistent cookies or other tracking devices to identify web visitors?
Upon logging into e–trak, a session cookie is created. The session cookie is eliminated once the web user ends his/her session and exits out of the web browser. Persistent cookies are not administered by this system.

[View other PIAs on IRS.gov](#)