

NOTE: The following reflects the information entered in the PIAMS website.

A. SYSTEM DESCRIPTION

Authority: Office of Management Budget (OMB) Memorandum (M) 03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 & PVR #10- Privacy Accountability and #21-Privacy Risk Management

Date of Approval: _____ PIA ID Number: **956**

1. What type of system is this? Modernized System

1a. Is this a Federal Information Security Management Act (FISMA) reportable system? Yes

2. Full System Name, Acronym, and Release/Milestone (if appropriate):

Voluntary Disclosure Program, e-trak VDP

2a. Has the name of the system changed? No

If yes, please state the previous system name, acronym, and release/milestone (if appropriate):

3. Identify how many individuals the system contains information on

Number of Employees: Under 50,000

Number of Contractors: Not Applicable

Members of the Public: Under 100,000

4. Responsible Parties:

NA

5. General Business Purpose of System

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 the Offshore Voluntary Disclosure Program and other Offshore Compliance Initiatives. 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. Due process is provided pursuant to 26 USC, 18 USC, and 31 USC.

6. Has a PIA for this system, application, or database been submitted previously to the Office of Privacy Compliance? (If you do not know, please contact *Privacy and request a search) Yes

6a. If **Yes**, please indicate the date the latest PIA was approved: 11/17/2011

6b. If **Yes**, please indicate which of the following changes occurred to require this update.

- System Change (1 or more of the 9 examples listed in OMB 03-22 applies) (refer to PIA Training Reference Guide for the list of system changes) No
 - System is undergoing Security Assessment and Authorization No
-

6c. State any changes that have occurred to the system since the last PIA

PIA is expiring in May, 2014

7. If this system has an Exhibit 53 or Exhibit 300 please provide the Unique Project Identifier (UPI) number (XXX-XX-XX-XX-XXXX-XX). Otherwise, enter the word 'none' or 'NA'. NA

B. DATA CATEGORIZATION

Authority: OMB M 03-22 & PVR #23- PII Management

8. Does this system collect, display, store, maintain or disseminate Personally Identifiable Information (PII)? Yes

8a. If **No**, what types of information does the system collect, display, store, maintain or disseminate?

9. Indicate the category that best describes the source that provides or originates the PII collected, displayed, stored, maintained or disseminated by this system. Most common categories follow:

Taxpayers/Public/Tax Systems Yes

Employees/Personnel/HR Systems Yes

Other Source:

Other No

10. Indicate all of the types of PII collected, displayed, stored, maintained or disseminated by this system. Then state if the PII collected is on the Public and/or Employees. Most common fields follow:

TYPE OF PII	Collected?	On Public?	On IRS Employees or Contractors?
Name	Yes	Yes	Yes
Social Security Number (SSN)	Yes	Yes	No
Tax Payer ID Number (TIN)	Yes	Yes	No
Address	Yes	Yes	No
Date of Birth	Yes	Yes	No

Additional Types of PII: No

No Other PII Records found.

10a. What is the business purpose for collecting and using the SSN?

SSN/EIN has to be used to recognize the taxpayers uniquely to determine the tax owned by them for unreported income from offshore taxpayer income as mandated by the IRS.

If you answered **Yes** to Social Security Number (SSN) in question 10, answer **10b**, **10c**, and **10d**.

10b. Cite the authority that allows this system to contain SSN's? (e.g. specific regulations, statutes, etc.)

SSNs are permissible from Internal Revenue Code (IRC) 6109, "Identifying Numbers" which requires individual taxpayers to include their SSNs on their income tax returns.

10c. What alternative solution to the use of the SSN has/or will be applied to this system? (e.g. masking, truncation, alternative identifier)

None, SSN/EIN has to be used to recognize the taxpayers uniquely to determine the tax owned by them for unreported income from offshore taxpayer income as mandated by the IRS.

10d. Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of Social Security Numbers on this system?

None

Describe the PII available in the system referred to in question 10 above.

Taxpayer's data is received via secure shared drive from the Criminal Investigations organization within the IRS and then entered into the e-trak application manually.

11. Describe in detail the system's audit trail. State what data elements and fields are collected. Include employee log-in information. If the system does not have audit capabilities, explain why an audit trail is not needed.

e-trak VDP application has full audit trail capabilities. The audit trail assures that those who use e-trak VDP only have permission to view and use the modules their role allows. The SA prepares and reviews monitoring reports based on Identity Theft and Incident Management (ITIM) established timeframes

11a. Does the audit trail contain the audit trail elements as required in current IRM 10.8.3 *Audit Logging Security Standards*? Yes

12. What are the sources of the PII in the system? Please indicate specific sources:

- a. IRS files and databases: No
If **Yes**, the system(s) are listed below:
No System Records found.
- b. Other federal agency or agencies: No
If **Yes**, please list the agency (or agencies) below:
- c. State and local agency or agencies: No
If **Yes**, please list the agency (or agencies) below:
- d. Third party sources: No
If yes, the third party sources that were used are:
- e. Taxpayers (such as the 1040): No
- f. Employees (such as the I-9): No
- g. Other: Yes If **Yes**, *specify*: Taxpayer data is received via secure shared drive from the Criminal Investigation organization within the IRS.

C. PURPOSE OF COLLECTION

Authorities: OMB M 03-22 & Internal Revenue Manual (IRM) 10.8.8, IT Security, Live Data Protection Policy & PVR #16, Acceptable Use

13. What is the business need for the collection of PII in this system? Be specific.

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 the tax owed.

D. PII USAGE

Authority: OMB M 03-22 & PVR #16, Acceptable Use

14. What is the specific use(s) of the PII?

To conduct tax administration	<u>Yes</u>	
To provide taxpayer services	<u>No</u>	
To collect demographic data	<u>No</u>	
For employee purposes	<u>No</u>	
Other:	<u>No</u>	<u><i>If other, what is the use?</i></u>

E. INFORMATION DISSEMINATION

Authority: OMB M 03-22 & PVR #14- Privacy Notice and #19- Authorizations

15. Will the information be shared outside the IRS? (for purposes such as computer matching, statistical purposes, etc.) No

15a. If yes, with whom will the information be shared? The specific parties are listed below:

	Yes/No	Who?	ISA OR MOU**?
Other federal agency (-ies)			
State and local agency (-ies)			
Third party sources			
Other:			

** Inter-agency agreement (ISA) or Memorandum of Understanding (MOU)

16. Does this system host a website for purposes of interacting with the public? No

17. Does the website use any means to track visitors' activity on the Internet?

If yes, please indicate means:

	YES/NO	AUTHORITY
Persistent Cookies	_____	_____
Web Beacons	_____	_____
Session Cookies	_____	_____
Other:	_____	_____

If other, specify:

F. INDIVIDUAL CONSENT

Authority: OMB M 03-22 & PVR #15- Consent and #18- Individual Rights

18. Do individuals have the opportunity to decline to provide information or to consent to particular uses of the information? Not Applicable

18a. If **Yes**, how is their permission granted?

19. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action? Not Applicable

19a. If **Yes**, how does the system ensure "due process"?

20. Did any of the PII provided to this system originate from any IRS issued forms? No

20a. If **Yes**, please provide the corresponding form(s) number and name of the form.

No forms found.

20b. If **No**, how was consent granted?

Written consent	_____	No
Website Opt In or Out option	_____	No
Published System of Records Notice in the Federal Register	_____	No
Other: <u>Taxpayer data is received via secure shared drive from the Criminal Investigation Division, Exchange of Information Office, or the Offshore Compliance Initiative Program within the IRS.</u>	_____	Yes

G. INFORMATION PROTECTIONS

Authority: OMB M 03-22 & PVR #9- Privacy as Part of the Development Life Cycle, #11- Privacy Assurance, #12- Privacy Education and Training, #17- PII Data Quality, #20- Safeguards and #22- Security Measures

21. Identify the owner and operator of the system: IRS Owned and Operated

21a. If Contractor operated, has the business unit provided appropriate notification to execute the annual security review of the contractors, when required?

22. The following people have use of the system with the level of access specified:

	Yes/No	Access Level
IRS Employees:	<u>Yes</u>	
Users		<u>Read Write</u>
Managers		<u>Read Only</u>
System Administrators		<u>Read Write</u>
Developers		<u>Read Write</u>
Contractors:	<u>No</u>	
Contractor Users		<u></u>
Contractor System Administrators		<u></u>
Contractor Developers		<u></u>
Other:	<u>No</u>	<u></u>

If you answered yes to contractors, please answer **22a.** (All contractor/contractor employees must hold at minimum, a "Moderate Risk" Background Investigation if they have access to IRS owned SBU/PII data.)

22a. If the contractors or contractor employees act as System Administrators or have "Root Access", does that person hold a properly adjudicated "High Level" background investigation?

23. How is access to the PII determined and by whom?

e-trak VDP administrator of the application will create and assign role based user accounts to designate/control user access to PII within the application.

24. How will each data element of SBU/PII be verified for accuracy, timeliness, and completeness?

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. The SA prepares and reviews monitoring reports based on ITIMs established timeframes to validate/verify data. PII data is not collected by the application as data elements.

25. Are these records covered under the General Records Schedule (GRS), or have a National Archives and Records Administration (NARA) archivist approved a Record Control Schedule (RCS) for the retention and destruction of official agency records stored in this system? No

25a. If **Yes**, how long are the records required to be held under the corresponding RCS and how are they disposed of? In your response, please include the complete IRM number 1.15.XX and specific item number and title.

A request for records disposition authority for e-trak VDP module 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 inputs, system data, outputs and system documentation will be published in IRS Document 12990, exact Records Control Schedule and item number to be determined.

If **No**, how long are you proposing to retain the records? Please note, if you answered no, you must contact the IRS Records and Information Management Program to initiate records retention scheduling before you dispose of any records in this system.

A request for records disposition authority for e-trak VDP module 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 inputs, system data, outputs and system documentation will be published in IRS Document 12990, exact Records Control Schedule and item number to be determined.

26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.

Users are assigned to specific modules of the application and specific roles within the modules and thus, only the appropriate PII data is available to those individuals to perform their duties after receiving appropriate approval and authorization through OL-5081. Additionally, accounts follow the principle of least privilege which provide them the least amount of access to PII data that is required to perform their business function

26a. Next, explain how the data is protected in the system at rest, in flight, or in transition.

Data at rest is stored securely at the database layer of the database server. E-trak protects data at rest as follows: E-trak, in accordance with the IRM 10.8.1.5.6, has employed the following due diligence methods for protecting data at rest that resides on the servers: E-trak does not utilize any shares or shared drives. E-trak enforces least privileges through Role Based Access Controls that limit users to only the data necessary to perform their assigned duties. E-trak reports are printed in accordance with business need. Reports are handled appropriately in accordance with organizational policies. E-trak has had a risk assessment conducted. Security Assessment Services has completed a Security Impact Analysis as part of the current SA&A cycle. The e-trak SSP is being updated as part of the current SA&A to reflect the encryption utilized by the application to protect SBU data. Physical security is inherited for e-trak at an organizational level. Physical security requirements are detailed in the IRS Facility Security Plan. Within our security accreditation, the protection of data at rest is inherited from Security Control (SC) - 28: Protection of Information Act Rest. The GSSs MITS-24, MITS-30 and MITS-32 inherit the responsibility for ensuring the information system protects the confidentiality and integrity of information at rest.

27. Has a risk assessment (e.g., SA&A) been conducted on the system to ensure that appropriate security controls have been identified and implemented to protect against known risks to the confidentiality, integrity and availability of the PII? Yes

28. Describe the monitoring/evaluating activities undertaken on a regular basis to ensure that controls continue to work properly in safeguarding the PII.

All account access to the system is granted through the OL5081 authorization process thus ensuring that authorization is granted from appropriate designated officials and that identifiers are securely distributed to the individuals requesting access. E-trak regularly runs audits to determine accounts that no longer need access to PII or are inactive. Per IRM 10.8.1.5.1.3, after 120 days of inactivity, the user's account will be disabled, but not removed from the system. After 365 days of inactivity, the account will be automatically deleted. Disabled or deleted accounts require that the user go through the OL5081 process to regain access to the system. In addition, the SSP is reviewed annually during continuous monitoring initiatives, and updated at least every three years or whenever there are significant changes to the system.

29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 - *IT Security, Live Data Protection Policy*? Not Applicable

29a. Has approval been received from the Office of Privacy Compliance to use Live Data in testing (*if appropriate*)?

29b. If you have received permission from the Office of Privacy Compliance to use Live Data, when was the approval granted?

H. PRIVACY ACT & SYSTEM OF RECORDS

Under the statute, any employee who knowingly and willfully maintains a system of records without meeting the Privacy Act notice requirements is guilty of a misdemeanor and may be fined up to \$5000.

Authority: OMB M 03-22 & Privacy Act, 5 U.S.C. 552a (e) (4) & PVR #13-Transparency

30. Are 10 or more records containing PII maintained/stored/transmitted through this system? Yes

31. Are records on the system retrieved by any identifier for an individual? (Examples of identifiers include but are not limited to Name, SSN, Photograph, IP Address) Yes

31a. If **YES**, the System of Records Notice(s) (SORN) published in the Federal Register adequately describes the records as required by the Privacy Act? Enter the SORN number and the complete name of the SORN.

SORNS Number

SORNS Name

Treas/IRS 42.021 Compliance Programs and Project Files

Treas/IRS 42.001 Exam Administrative File

Treas/IRS 42.017 International Enforcement Program Files

Treas/IRS 34.037 IRS Audit Trail and Security Records System

Treas/IRS 42.031 Anti-Money Laundering IBank Secrecy Act (BSA) and

I. ANALYSIS

Authority: OMB M 03-22 & PVR #21- Privacy Risk Management

32. What choices were made or actions taken regarding this IT system or collection of information as a result of preparing the PIA?

Resulted in the removal of PII from the system (e.g., SSN use reduced/eliminated)

No

Provided viable alternatives to the use of PII within the system

No

New privacy measures have been considered/implemented

No

Other:

No

32a. If **Yes** to any of the above, please describe:

Current PIA is due to expire in May, 2014.