Date of Approval: April 28, 2017 PIA ID Number: **2565**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Voluntary Disclosure Program, e-trak VDP

2. Is this a new system? No

2a. If **no**, is there a PIA for this system? Yes

If **yes**, enter the full name, acronym, PIA ID Number and milestone of the most recent PIA.

Voluntary Disclosure Program, e-trak VDP, #884

Next, enter the **date** of the most recent PIA. 7/2/2014

Indicate which of the following changes occurred to require this update (check all that apply).

No	Addition of PII
No	Conversions
No	Anonymous to Non-Anonymous
No	Significant System Management Changes
No	Significant Merging with Another System
No	New Access by IRS employees or Members of the Public
No	Addition of Commercial Data / Sources
No	New Interagency Use
No	Internal Flow or Collection

Were there other system changes not listed above? No

If yes, explain what changes were made.

3. Check the current ELC (Enterprise Life Cycle) Milestones (select all that apply)

No	Vision & Strategy/Milestone 0
No	Project Initiation/Milestone 1
No	Domain Architecture/Milestone 2
No	Preliminary Design/Milestone 3
No	Detailed Design/Milestone 4A
No	System Development/Milestone 4B
No	System Deployment/Milestone 5
Yes	Operations & Maintenance (i.e., system is currently operational)

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

A.1 General Business Purpose

5. What is the general business purpose of this system? Provide a clear, concise description of the system, application or database, the reason for the system, and the benefits to the IRS to use the information, and how the information will be used.

The e-Trak (Voluntary Disclosure Program) VDP system provides the Large Business & International organization the flexibility it requires to store, retrieve, update, and track taxpayer data relative to the Offshore Voluntary Disclosure Program and other Offshore Compliance Initiatives. The main purpose of the application is to gather information from examiners concerning what they see during their offshore certification or examination. The focus is on the banks, countries, and promoters involved in offshore wealth management. This information is used to analyze offshore trends, identify countries and banks that are most involved in offshore asset movement, and to discover new offshore schemes and promotions. e-trak VDP is also used to generate statistics & reports for LBI management, the Department of Justice, and for Congressional inquiries. Due process is provided pursuant to 26 USC,18 USC, and 31 USC.

B. PII DETAIL

6. Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any type of Sensitive but Unclassified (SBU) or Personally Identifiable Information (PII)? Yes

6a. If **yes**, does the system use, collect, receive, display, store, maintain, or disseminate Social Security Numbers (SSN s) or tax identification numbers (i.e. last 4 digits, etc.)? Yes

If **yes**, check who the SSN (or tax identification number) is collected on.

Yes On Primary Yes On Spouse No On Dependent

If **yes**, check all types SSN s (or tax identification numbers) that apply to this system:

Yes	Social Security Number (SSN)
Yes	Employer Identification Number (EIN)
Yes	Individual Taxpayer Identification Number (ITIN)
No	Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
No	Practitioner Tax Identification Number (PTIN)

Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN s (or tax identification numbers).

The SSN/TIN must be used to identify taxpayers and properly assess tax/penalties owed due to unreported offshore transactions, as mandated by the IRS. The Office of Management and Budget memorandum M-07-12 requires that federal agencies develop a mitigation or elimination strategy for systems that use SSNs, which the Service continues to develop strategies to meet. An exception to that requirement is when the SSN is uniquely needed to identify a user's record. The e-trak VDP requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer at this time. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns.

6b. Does this system contain other (non-SSN) PII that it uses, collects, receives, displays, stores, maintains, or disseminates? (i.e. Names, addresses, etc.) Yes

If **yes**, specify the information.

Selected	PII Element	On Primary	On Spouse	On Dependent
Yes	Name	Yes	Yes	No
Yes	Mailing address	No	No	No

Yes	Phone Numbers	No	No	No
No	E-mail Address	No	No	No
Yes	Date of Birth	Yes	Yes	No
No	Place of Birth	No	No	No
Yes	SEID	No	No	No
No	Mother's Maiden Name	No	No	No
No	Protection Personal Identification Numbers (IP PIN)	No	No	No
No	Internet Protocol Address (IP Address)	No	No	No
No	Criminal History	No	No	No
No	Medical Information	No	No	No
No	Certificate or License Numbers	No	No	No
No	Vehicle Identifiers	No	No	No
No	Passport Number	No	No	No
No	Alien (A-) Number	No	No	No
No	Financial Account Numbers	No	No	No
No	Photographic Identifiers	No	No	No
No	Biometric Identifiers	No	No	No
No	Employment (HR) Information	No	No	No
Yes	Tax Account Information	Yes	Yes	No

6c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? Yes

If **yes**, select the types of SBU

Selected	SBU Name	SBU Description
No	Agency Sensitive Information	Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission
No	Procurement sensitive data	Contract proposals, bids, etc.
No	Official Use Only (OUO) or Limited Official Use (LOU)	Information designated as OUO or LOU is information that: is exempt under one of the statutory Freedom of Information Act exemptions; is prohibited by other laws or regulations; would significantly impede the agency in carrying out a responsibility or function; or would constitute an unwarranted invasion of privacy.
No	Proprietary data	Business information that does not belong to the IRS
Yes	Protected Information	Information which if modified, destroyed or disclosed in an unauthorized manner could cause: loss of life, loss of property or funds by unlawful means, violation of personal privacy or civil rights, gaining of an unfair procurement advantage by contractors bidding on government contracts, or disclosure of proprietary information entrusted to the Government
No	Physical Security Information	Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities
No	Criminal Investigation Information	Information concerning IRS criminal investigations or the agents conducting the investigations.

6d. Are there other types of SBU/PII used in the system? No

6e. Cite the authority for collecting SBU/PII (including SSN if relevant)

Yes	PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)

Yes	SSN for tax returns and return information is Internal Revenue Code Section 6109
No	SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
No	PII for personnel administration is 5 USC
Yes	PII about individuals for Bank Secrecy Act compliance 31 USC
No	Information by CI for certain money laundering cases may be 18 USC

6f. Has the authority been verified with the system owner? Yes

B.1 BUSINESS NEEDS AND ACCURACY

7. Explain the detailed business needs and uses for the SBU/PII, and how the SBU/PII is limited only to that which is relevant and necessary to meet the mission requirements of the system. If SSNs (or tax identification numbers) are used, explicitly explain why use of SSNs meets this criteria. Be specific.

The SSN/TIN must be used to identify taxpayers and properly assess tax/penalties owed due to unreported offshore transactions, as mandated by the IRS. The SSN/TIN is also required in order to verify that taxpayers continue to properly report their offshore transactions. All fields (name, addresses and any taxpayer information) were vetted through a team of offshore tax experts and deemed necessary to understanding what has occurred, what is owed, where unreported offshore transactions have taken place, who promoted them, and where they might occur in the future. 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.

8. How is the SBU/PII verified for accuracy, timeliness, and completeness? Explain how steps are taken to ensure that all information maintained by the system that is used by IRS to make any adverse determination about an individual's rights, benefits, and/or privileges is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination

All cases entered into the system are either certified by or examined by a Revenue Agent or Tax Examiner. The data is verified for accuracy by the Agent/Examiner. There are internal programming consistency checks and record counts to validate the data that is loaded into the e-trak VDP system is accurate. The data that e-trak receives is from internal IRS systems which are deemed reliable and the data is validated for accuracy by the system sending the data as described in that system's PCLIA. The system is not used to make adverse determinations about an individual's rights, benefits, and/or privileges. Any determinations made are validated during examination and collection process and the taxpayer has appeal rights for any determinations made from the data.

C. PRIVACY ACT AND SYSTEM OF RECORDS

9. Are 10 or more records containing SBU/PII maintained, stored, and/or transmitted by or through this system? Yes

9a. If **yes**, are records in the system retrieved by any personal identifier (e.g., name, SSN, Photograph, IP Address) for an individual? Yes

If **yes**, is there a System of Records Notice(s) or SORNs that addresses the PII records in this system? Yes

If **yes**, enter the SORN number(s) and the complete the name of the SORN.

SORNS Number	SORNS Name
Treas/lRS 42.021	Compliance Programs and Project Files
Treas/lRS 42.001	Exam Administrative File
Treas/lRS 42.017	lnternational Enforcement Program Files
Treas/lRS 34.037	IRS Audit Trail and Security Records System
Treas/lRS 42.031	Anti-Money Laundering IBank Secrecy Act (BSA)

If **yes**, does the System of Records Notice(s) (SORN) published in the Federal Register adequately describe the records as required by the Privacy Act? Yes

D. RESPONSIBLE PARTIES

10. Identify the individuals for the following system roles. ## Official Use Only

E. INCOMING PII INTERFACES

11. Does the system receive SBU/PII from other system or agencies? No

F. PII SENT TO EXTERNAL ORGANIZATIONS

12. Does this system disseminate SBU/PII? No

G. PRIVACY SENSITIVE TECHNOLOGY

13. Does this system use social media channels? No

14. Does this system use privacy-sensitive technologies such as mobile, cloud, global position system (GPS), biometrics, RFID, etc.? No

15. Does the system use cloud computing? No

16. Does this system/application interact with the public? No

H. INDIVIDUAL NOTICE AND CONSENT

17. Was/is notice provided to the individual prior to collection of information? No

17b. If **no**, why not? If information is not collected directly from an individual, please discuss the factors considered in deciding to collect information from third party sources.

Information is not collected directly from individuals. Taxpayer data is received from the IRS Criminal Investigation Division, Exchange of Information Office (EOI), or the Offshore Compliance Initiative Program. The information collected pertains to unreported offshore transactions. It is either provided voluntarily to Criminal Investigation in exchange for participating in the Offshore Voluntary Disclosure Initiative, through EOI as part of an agreement with other governments, or as part of a court enforced John Doe summons.

18. Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information? No

18b. If no, why not? Information is not collected directly from individuals. Taxpayer data is received from the IRS Criminal Investigation Division, Exchange of Information Office (EOI), or the Offshore Compliance Initiative Program. The information collected pertains to unreported offshore transactions. It is either provided voluntarily to Criminal Investigation in exchange for participating in the Offshore Voluntary Disclosure Initiative, through EOI as part of an agreement with other governments, or as part of a court enforced John Doe summons.

19. How does the system or business process ensure due process regarding information access, correction and redress?

Cases are either certified or examined by IRS Revenue Agents. Taxpayers are given an opportunity to discuss the information at that time. Taxpayers who are examined are given full appeal rights, as provided by law. All individuals have the right to decline to provide information. However, they may be subject to Examination or Deficiency procedures, at which time they are provided applicable notices, such as Your Appeals Rights and How to Prepare a Protest.

I. INFORMATION PROTECTION

20. Identify the owner and operator of the system (could be IRS owned and Operated; IRS owned, contractor operated; contractor owned and operated)

IRS Owned and Operated

21. The following people have access to the system with the specified rights:

IRS Employees? Yes

IRS Employees?	Yes/No	Access Level(Read Only/Read Write/ Administrator)
Users	Yes	Read and Write
Managers	Yes	Read-Only
Sys. Administrators	Yes	Administrator
Developers	Yes	Read And Write

Contractor Employees? No

21a. How is access to SBU/PII determined and by whom? All requests for access go through the ol5081 process. Potential users must be approved by their manager and then the e-trak administrator. A potential user must submit a request for access via IRS On–Line application 5081 (OL5081) to their local management for approval consideration. Users are not permitted access without a signed 5081 form from an authorized management official. Specific permissions (Read, Write, Modify, Delete, and/or Print) are defined on the OL5081 form and set (activated) by the System Administrator prior to the user being allowed access. User privileges and user roles determine the types of data that each user has access to.

Management monitors system access and removes permissions when individuals no longer require access. The e-trak VDP administrator creates and assigns "role based" user accounts to designate, control, & limit user access to PII within the application. Accounts follow the principle of "least privilege," which provides users with the least amount of access to PII data that is required to perform their business function.

21b. If computer matching occurs, can the business owner certify that it meets requirements of IRM 11.3.39 Disclosure of Official Information, Computer Matching & Privacy Protection Act ? Not Applicable

I.1 RECORDS RETENTION SCHEDULE

22. 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

22b. 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.

I.2 SA&A OR ECM-R

23. Has the system been through SA&A (Security Assessment and Authorization) or ECM-R (Enterprise Continuous Monitoring Reauthorization)? Yes

23a. If **yes**, what date was it completed? 1/13/2017

23.1 Describe in detail the system s audit trail. e-trak VDP application has full audit trail capabilities. Amongst other things, the system records: logins, logouts, account creation, account deletions, timeouts, & locked accounts. 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. E-trak regularly runs audits to determine accounts that no longer need access to PII or our 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.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? Yes

24b. If **yes**, Is the test plan in process or completed: Completed

24.3 If **completed/ or in process,** describe what testing and validation activities have been conducted or are in progress to verify and validate that the applicable Privacy Requirements (listed in header) have been met?
Create test cases and test scripts for security and privacy requirements. These test cases and test scripts are to validate and verify user access control procedures, ensure strict confidentiality, use of data, and accountability.

24b.1. If **completed**, where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)? System Test Plan, Unit test Plan, User Acceptance testing, test cases and test scripts. The plans are stored in DocIT. The test cases, test scripts and test plans are generated and stored in CLM Collaborate Lifecycle Management Quality Manager Tool.

24b.2. If **completed**, were all the Privacy Requirements successfully tested? Yes

24.2 If **completed**, are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved? No

K. SBU Data Use

25. Does this system use, or plan to use SBU Data in Testing? No

L. NUMBER AND CATEGORY OF PII RECORDS

26. Identify the number of individual records in the system for each category:

26a. IRS Employees: Under 50,000
26b. Contractors: Not Applicable
26c. Members of the Public: Not Applicable
26d. Other: No

M. CIVIL LIBERTIES

27. Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment? No

28. Is the system information used to conduct data-mining as defined in the *Implementing the 9/11 Commission Recommendations Act of 2007, Public Law 110-53, Section 804?* No

29. Will this system have the capability to identify, locate, and monitor individuals or groups of people? No

N. ACCOUNTING OF DISCLOSURES

30. Does the system include or require disclosure of tax or employee information to anyone other than IRS employees in the performance of their duties, or to the person to whom the information pertains or to a 3rd party pursuant to a Power of Attorney, tax or Privacy Act consent? No

End of Report