Date of Approval: **March 29, 2020**

PIA ID Number: **4854**

SYSTEM DESCRIPTION

Enter the full name and acronym for the system, project, application and/or database.

Voluntary Disclosure Program, e-Trak VDP

Is this a new system?

No

Is there a PCLIA for this system?

Yes

What is the full name, acronym and milestone of the most recent PCLIA?

Voluntary Disclosure Program, e-Trak VDP, #2565

What is the approval date of the most recent PCLIA?

5/2/2017

Changes that occurred to require this update:

Expiring PCLIA

Were there other system changes not listed above?

No

What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym.

AD Compliance Governance Board

Current ELC (Enterprise Life Cycle) Milestones:

System Development/Milestone 4B

Operations & Maintenance (i.e. system is currently operational)

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

Yes

GENERAL BUSINESS PURPOSE

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 Large Business & International (LBI) management, the Department of Justice, and for Congressional inquiries. Due process is provided pursuant to Title 26 United States Code (USC), Title 18 USC, and Title 31 USC.

PII DETAILS

Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any other type of Sensitive but Unclassified (SBU) information or PII such as information about IRS employees or outside stakeholders?

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

What types of tax identification numbers (TIN) apply to this system?

Social Security Number (SSN)

List the approved Treasury uses of the SSN:

Interfaces with external entities that require the SSN

Statistical and other research purposes

Law enforcement and intelligence purposes

Explain why the authorized use(s) above support the new or continued use of SSNs (or tax identification numbers)

The SSN/TIN is 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 needed to verify that taxpayers continue to properly report their offshore transactions. The e-trak VDP requires the use of SSN/TIN's because no other identifier can be used to uniquely identify a taxpayer at this time.

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 Circular A-130 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/TIN is uniquely needed to identify a user's record. The e-trak VDP requires the use of SSN/TIN's because no other identifier can be used to uniquely identify a taxpayer at this time. SSN/TIN's are permissible under Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns.

Employer Identification Number

Does this system use, collect, receive, display, store, maintain or disseminate other (non-SSN) PII (i.e. names, addresses, etc.)?

Yes

Specify the PII Elements:

Name

Mailing address

Phone Numbers

Date of Birth

Standard Employee Identifier (SEID)

Passport Number

Financial Account Numbers

Tax Account Information

Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?

Yes

Specify the types of SBU from the SBU Types List

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

Are there other types of SBU/PII used in the system?

No

Cite the authority for collecting SBU/PII (including SSN if relevant

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

SSN for tax returns and return information is Internal Revenue Code Section 6109

PII about individuals for Bank Secrecy Act compliance 31 USC

Information by CI for certain money laundering cases may be 18 USC

Has the authority been verified with the system owner?

Yes

BUSINESS NEEDS AND ACCURACY

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.

How is the SBU/PII verified for accuracy, timeliness and completion?

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.

PRIVACY ACT AND SYSTEM OF RECORDS

The Privacy Act requires Federal agencies that maintain a system of records to publish systems of records notices (SORNs) in the Federal Register for records from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence. The Privacy Act also provides for criminal penalties for intentional noncompliance.

Does your application or this PCLIA system pertain to a group of any record from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence? An identifier may be a symbol, voiceprint, SEID, or other personal identifier that is used to retrieve information.

Yes

Identify the Privacy Act SORN(s) that cover these records.

lRS 42.021 Compliance Programs and Project Files

lRS 42.001 Examination Administrative Files

lRS 42.017 International Enforcement Program Information Files

lRS 34.037 Audit Trail and Security Records

lRS 42.031 Anti-Money Laundering/Bank Secrecy Act and Form 8300

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

Official Use Only

INCOMING PII INTERFACES

Does the system receive SBU/PII from other systems or agencies?

Yes

Does the system receive SBU/PII from IRS files and databases?

Yes

Enter the files and databases:

System Name: Integrated Data Retrieval System (IDRS)
Current PCLIA: Yes
Approval Date: 10/1/2018
SA&A: Yes
ATO/IATO Date: 11/20/2018

System Name: Exchange of Information (EOI)- (Issue Management System) (IMS)
Current PCLIA: Yes
Approval Date: 9/3/2019
SA&A: Yes
ATO/IATO Date: 12/8/2018

System Name: Audit Information Management System (AIMS)
Current PCLIA: Yes
Approval Date: 11/20/2018
SA&A: Yes
ATO/IATO Date: 2/5/2020

System Name: Examination Returns Control System (ERCS)
Current PCLIA: Yes
Approval Date: 2/7/2017
SA&A: Yes
ATO/IATO Date: 11/12/2019

Does the system receive SBU/PII from other federal agency or agencies?

Yes

For each federal interface, identify the organization that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Name: Department of Justice Swiss Bank Program
Transmission Method: Electronic Fund Transfer (EFT)
ISA/MOU: Yes

Does the system receive SBU/PII from State or local agency (-ies)?

No

Does the system receive SBU/PII from other sources?

No

Does the system receive SBU/PII from Taxpayer forms?

Yes

Please identify the form number and name:

Form Number: Form 114 Form Name: Report of Foreign and Financial Bank Accounts

Form Number: Form 14457 Form Name: Voluntary Disclosure Practice Preclearance Request and Application

Does the system receive SBU/PII from Employee forms (e.g. the I-9)?

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

No

PRIVACY SENSITIVE TECHNOLOGY

Does this system use social media channels?

No

Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.?

No

Does the system use cloud computing?

No

Does this system/application interact with the public?

No

INDIVIDUAL NOTICE AND CONSENT

Was/is notice provided to the individual prior to collection of information?

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.

Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information?

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.

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.

INFORMATION PROTECTION

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

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

IRS Employees

Users: Read Write

Managers: Read Only

System Administrators: Administrator

Developers: Read Write

How is access to SBU/PII determined and by whom?

All requests for access go through the online 5081 (ol5081) process. Potential users must be approved by their manager and then the e-Trak administrator. Potential users must submit a request for access via the ol5081 process 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.

RECORDS RETENTION SCHEDULE

Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) approved a Records Control Schedule (RCS, IRS Document 12990) for the retention and destruction of official agency records stored in this system?

Yes

How long are the records required to be held under the corresponding GRS or RCS, and how are they disposed of? In your response, please provide the GRS or RCS chapter number, the specific item number, and records series title.

RCS 22 Item 54-Offshore Compliance Initiative (OCI). (A) Inputs: Taxpayer information is received from sources external to IRS. AUTHORIZED DISPOSITION Delete/Destroy when 20 years old, or when no longer needed for legal, audit or other operational purposes. (B) System Data: Taxpayer Information in the OCI database includes account name, credit card number, all persons with signature authority over account, credit card transaction data, and other information used to determine if the taxpayer has reported all income that may be held in offshore accounts. AUTHORIZED DISPOSITION Delete/Destroy when 20 years old, or when no longer needed for legal, audit or other operational purposes. (C) Outputs: Outputs include ad hoc queries of names or credit card numbers held in the system to do further research. AUTHORIZED DISPOSITION Delete/Destroy when no longer needed for legal, audit or other operational purposes. (D) System Documentation: Owners Manual, User Manual, Data Dictionary, Software Design Description, Software Requirements, et al. AUTHORIZED DISPOSITION Delete/Destroy when superseded or 5 years after the system is terminated, whichever is sooner.

SA&A OR ASCA

Has the system been through SA&A (Security Assessment and Authorization) or ASCA (Annual Security Control Assessment)?

Yes

What date was it completed?

12/12/2019

Describe 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 System Administrator (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.

PRIVACY TESTING

Does the system require a System Test Plan?

Yes

Is the test plan completed?

Yes

Where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)?

The test cases, test scripts and test plans are generated and stored in Collaborate Lifecycle Management Quality Manager Tool.

Were all the Privacy Requirements successfully tested?

Yes

Are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved?

No

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?

System Test Plan, Unit test Plan, User Acceptance testing, test cases and test scripts.

SBU DATA USE

Does this system use, or plan to use SBU Data in Testing?

No

NUMBER AND CATEGORY OF PII RECORDS

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

IRS Employees: Under 50,000

Contractors: Not Applicable

Members of the Public: Under 100,000

Other: No

CIVIL LIBERTIES

Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment?

No

Is the system information used to conduct 'data-mining' as defined in the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?

No

Will this system have the capability to identify, locate, and monitor individuals or groups of people?

No

Does computer matching occur?

No

ACCOUNTING OF DISCLOSURES

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