Date of Approval: **August 01, 2019**

PIA ID Number: **4158**

SYSTEM DESCRIPTION

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

e-Trak FBAR, e-Trak FBAR

Is this a new system?

Yes

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

Compliance Governance Board

Current ELC (Enterprise Life Cycle) Milestones:

System Development/Milestone 4B

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.

Title 31 of the United States Code (USC) Section 5314 requires individuals who have a financial interest in or signature or other authority over a foreign financial account, including a bank account, brokerage account, mutual find, trust, or other type of foreign financial account, exceeding certain thresholds, to annually file a Foreign Bank Account Report (FBAR), electronic Financial Crimes and Enforcement Network (FinCEN) Form 114. Internal Revenue Service has been delegated enforcement authority for FBAR compliance. The purpose of the e-Trak FBAR Penalty Database is to track cases subject to examination for possible FBAR violations. The database tracks the filer by name, address, and taxpayer identification number (TIN). It also tracks the disposition of the examination. e-Trak FBAR tracks activity as described in IRM 4.26.16 and 4.26.17. The database is also used to assess FBAR penalties, create demand letters (bill the taxpayer), and track penalty payments.

The e -Trak system is a web-based application which provides a centralized database for entering and monitoring. e-Trak allows for the generation and downloading of detailed and summary reports. e-Trak FBAR will be used to monitor and report enforcement efforts.

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:

Legal/statutory basis (e.g. where collection is expressly required by statute)

When there is no reasonable alternative means for meeting business requirements

Law enforcement and intelligence purposes

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

SSNs are needed for reporting and administrative records pertaining to the examination enforcement and collection records.

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

There are no current plans to eliminate the use of SSNs. The Office of Management and Budget 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 is uniquely needed to identify a user's record. SSNs are permissible under Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns.

Employer Identification Number

Other Taxpayer 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

E-mail Address

Standard Employee Identifier (SEID)

Internet Protocol Address (IP Address)

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 (SBUList)

Agency Sensitive Information - Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission

Proprietary data - Business information that does not belong to the IRS

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

Yes

Describe the other types of SBU/PII that are applicable to this system.

Examples of other types of SBU/PII used in the system includes: Employee Standard Employee Identifier (SEID), employee name, employee badge number, employee work phone number, employee work fax number, and employee work address. Other SBU/PII applicable to this system includes: names of foreign banks/institutions/agent(s), foreign account numbers, power of attorney name, and power of attorney address. The system also tracks disposition of the examinations, is used to create demand letters(bills), and to track penalty payments.

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 for personnel administration is 5 USC

PII about individuals for Bank Secrecy Act compliance 31 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.

SBU/PII is limited to that which is relevant and necessary to meet the mission of reporting and recording administrative records pertaining to FBAR enforcement. There are no direct data feeds into or out of the system. The database tracks the filer by name, address, and taxpayer identification number (TIN). It also tracks the disposition of the examination. This information is also required to prepare referrals to Department of Justice (DOJ) and/or Bureau of The Fiscal Service (BFS) as required by law. The information will also be used to prepare reports to Financial Crimes and Enforcement Network (FinCEN) and various inter-agency agreements including information shared with other governmental entities in accordance with applicable agreements. The e-Trak FBAR system requires the use of TINs because no other identifier can be used to uniquely identify a taxpayer. The Report of Foreign Bank and Financial Accounts requires a TIN.

Other types of SBU/PII used in the system includes: Employee Standard Employee Identifier (SEID), employee name, employee badge number, employee work phone number, employee work fax number, and employee work address. Other SBU/PII applicable to this system includes: names of foreign banks/institutions/agent(s), foreign account numbers, power of attorney name, and power of attorney address.

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

The e-Trak FBAR data system contains input masks validation tools, and other electronic checks/balances to ensure data input is accurate. Data input is tracked in audit logs which can be used for verification of timeliness and completeness.

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.

IRS 34.037	Audit Trail and Security Records System
IRS 42.031	Anti-Money Laundering/Bank Secrecy Act (BSA) and Form 8300

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

For 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: Examination Returns Control System (ERCS)

Current PCLIA: Yes

Approval Date: 2/7/2017

SA&A: Yes

ATO/IATO Date: 6/7/2019

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

No

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

No

Does the system receive SBU/PII from other sources?

Yes

Identify the source that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name: Electronic Financial Crimes and Enforcement Network (FinCEN) Form 114

Transmission Method: Input into e-trak by users

ISA/MOU   No

Does the system receive SBU/PII from Taxpayer forms?

No

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

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

Yes

Does this system disseminate SBU/PII to other IRS Systems?

No

Does this system disseminate SBU/PII to other Federal agencies?

Yes

Identify the full names of the federal agency(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) / Memorandum of Understanding (MOU).

Organization Name: US Treasury Financial Crimes Enforcement Network (FinCEN)

Transmission Method: Manual Export

ISA/MOU Yes

Organization Name: US Treasury Bureau of the Fiscal Service (BFS)

Transmission Method: Manual Export

ISA/MOU No

Organization Name: US Department of Justice

Transmission Method: Manual Export

ISA/MOU No

Identify the authority

Treasury .009 Treasury Fiscal Service Systems

Identify the Routine Use in the applicable SORN (or Privacy Act exception)

The Treasury Integrated Financial Management and Revenue System is to account for and control appropriated resources; maintain accounting and financial information associated with the normal operations of government organizations such as billing and follow-up, for paying creditors, to account for goods and services provided and received, to account for monies paid and received, process travel authorizations and claims, process training claims, and process employee claims for lost or damaged property. The records management and statistical analysis subsystems provide a data source for the production of reports, statistical surveys, documentation and studies required for integrated internal management reporting of costs associated with the Department's operation.

For what purpose?

Referral of FBAR cases to BFS for collection enforcement services, Referral of FBAR cases to Department of Justice for enforcement purposes, and FBAR case reporting statistics to FinCEN.

Does this system disseminate SBU/PII to State and local agencies?

No

Does this system disseminate SBU/PII to IRS or Treasury contractors?

No

Does this system disseminate SBU/PII to other Sources?

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.

The Information is not collected directly from an individual. The information is used for law enforcement purposes, collecting the information directly from the individual is not practicable because it would notify them that they are under investigation and may cause them to alter their practices to avoid detection. Individuals provide information to FinCEN as required under 31 USC 5314.

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

No

Why not?

The system collects FBAR examination information as well as information provided by the entity via voluntary information filing as require under 31 USC 5314. The data contained is verified during the examination process as outlined in IRM 4.26.16 and IRM 4.26.17.

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

The system will allow affected parties the opportunity to clarify or dispute negative information that could be used against them. Due process is provided pursuant to 5 USC.

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 Write

System Administrators: Administrator

Developers: Administrator

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

The e-Trak BAR system utilizes the IRS On-Line application OL-5081 application to document approvals for access. Data access is granted on a need-to-know basis. A potential user must submit a request for access via IRS 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. Users are assigned to specific modules of the application and specific roles within the modules and 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 after receiving appropriate approval.

RECORDS SCHEDULE

Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) archivist 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.

GRS 4.2, items 030 and 130, DAA-GRS 2016-0002-0002 and DAA-GRS 2103-0007-0012 govern disposal of records.

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?

12/6/2018

Describe the system's audit trail.

e-Trak FBAR application has full audit trail capabilities. Amongst other things, the system records: logins, logouts, account creation, account deletions, timeouts, and locked accounts. The audit trail assures that those who use e-Trak only have permission to view and use the modules their role allows. The audit log events are captured in the database.

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)?

Posted in DocIT (Document repository system for Enterprise Life Cycle. Test cases and test results are kept in International Business Machine (IBM) Rational Collaborative Lifecycle Management (CLM).

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?

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. In addition, e-Trak system is currently in the Operations and Maintenance phase of its lifecycle. Continuous Monitoring (eCM) (now called Annual Security Control Assessment) occurs annually to ensure that controls remain in place to properly safeguard PII.

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?

Yes

Does the system have a process in place to account for such disclosures in compliance with IRC §6103(p) (3) (A) or Subsection (c) of the Privacy Act? Contact Disclosure to determine if an accounting is required.

Yes