Date of Approval: **November 25, 2020**

PIA ID Number: **5634**

## SYSTEM DESCRIPTION

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

ETRAK ROI UNIT REPORT AND TRACKING SYSTEM, ROIU-RTS SYSTEM

*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?*

ETRAK ROI UNIT REPORT AND TRACKING SYSTEM, ROIU-RTS SYSTEM, # 3136

*What is the approval date of the most recent PCLIA?*

1/19/2018

*Changes that occurred to require this update:*

Significant System Management Changes

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 Report of Investigations Unit (ROIU) e-trak system will provide a means for tracking and assigning Treasury Inspector General for Tax Administration (TIGTA) reports of investigation to business units within the Internal Revenue Service (IRS). It will also provide a reporting system to gather data (i.e. Subject Name, Place of Birth, Date of Birth, Physical Description of Subject, Gender, Social Security Number, Criminal Rap Sheet). Our e-trak system uses the before mentioned data as a records retention system. Doing away with our previous paper filing system. E-trak is a system based on MicroPact's entellitrak, a commercial off the shelf software (COTS) product. The e-Trak Safeguards tool help to satisfy the data and functional needs of case management and metrics reporting on a more robust, web-based platform.

## 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:*

Security Background Investigations

When there is no reasonable alternative means for meeting business requirements

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).*

System stores Reports of Investigations that may contain PII information listed above.

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

System stores Reports of Investigations that may contain PII information listed above. There is no immediate mitigation to eliminate this process.

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

Date of Birth

Place of Birth

Standard Employee Identifier (SEID)

Mother's Maiden Name

Criminal History

Medical Information

Certificate or License Numbers

Passport Number

Photographic Identifiers

Employment Information

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.*

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

Procurement sensitive data Contract proposals, bids, etc.

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.

Proprietary data Business information that does not belong to the IRS

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

Physical Security Information Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities

Criminal Investigation Information Information concerning IRS criminal investigations or the agents conducting the investigations.

*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

SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397

PII for personnel administration is 5 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 Report of Investigations Unit (ROIU) e-trak system tracks all case information using Treasury Inspector General for Tax Administration (TIGTA) case numbers. The ROIU scans Report of Investigations (ROI) from TIGTA into e-trak which is used as our record retention data base. It replaces our need for paper files. We will not refer TIGTA Report on Investigations (ROI)s concerning employee/non-employee misconduct through this e-trak system. We have a separate process to forward misconduct ROIs to the servicing LR offices and Business Units. Types of data contained in TIGTA Investigations: (i.e. Subject Name, Place of Birth, Date of Birth, Physical Description of Subject, Gender, Social Security Number, Criminal Rap Sheet, IRS Directory Information which contains SEID info).

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

For accuracy purposes the Report of Investigations Unit (ROIU) verifies if the Subjects are still employed by the Internal Revenue Service (IRS) and if so, we forward the Reports of Investigations accordingly by (i.e. sending them to Labor Relations or Business Unit). There is no need for us to verify the SBU/PII information, as we are merely processing and tracking the reports of investigation to ensure they reach the appropriate business unit or LR area. All information is shared on a need-to-know basis within the IRS.

## 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 00.001 Correspondence Files and Correspondence Control Files

## 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?*

No

*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: Office of Personnel Management
Transmission Method: MAIL
ISA/MOU: Yes

Name: DEPARTMENT OF TREASURY
Transmission Method: SHAREPOINT
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?*

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?*

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.*

We do not collect the SBU/PII information. That is the role and responsibility of the Treasury Inspector General for Tax Administration (TIGTA). IRS policy allows individuals whose data is in the system the opportunity to clarify or dispute negative determinations through the appeals process.

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

No

*Why not?*

ETAK ROI does not directly provide individuals the opportunity to decline from providing information and/or from consenting to particular uses of the information. Notice, consent and due process are provided in the tax forms instructions filed by the taxpayer, and pursuant to 5 USC. We do not collect the SBU/PII information. The TIGTA collects the information and forwards it to the IRS in the complaint or allegation.

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

We do not collect the SBU/PII information. The TIGTA collects the information and forwards it to the IRS in the complaint or allegation. We follow all IRS procedures and security guidelines for safeguarding SBU/PII information. IRS policy allows individuals whose data is in the system the opportunity to clarify or dispute negative determinations through the appeals process." We share the information within the agency, only on a need-to-know basis. This is a FISMA reportable system.

# 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: Read Write

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

The EIB Chief and the ECCO Associate Director determine access to this ROIU system. Access is limited to the ROI Unit staff, the EIB Chief, and the ECCO Associate Director. The ROI Unit staff requires access to process and track the reports of investigation. The EIB Chief and the ECCO Associate Director require access for reporting and oversight purposes. Access control is managed through the OL5081 system is protected from non-authorized users Accountability. 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 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.*

All records housed in the eTrak ROI Unit Report and Tracking system will be erased or purged from the system in accordance with approved retention periods. It is the official repository for data and documents and has National Archives approval to affect data disposition. Any records generated and maintained by the system will be managed according to requirements under IRM 1.15.1 and 1.15.6, and will be destroyed using IRS General Records Schedule (GRS) 2.2, Item 010, and as coordinated with the IRS Records and Information Management (RIM) Program and IRS Records Officer.

## 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?*

10/21/2020

*Describe the system's audit trail.*

Per the IT point-of-contact, the audit trail will collect the following information: user log-in information; created and deleted activities; log-out details; the information collected on who performed the activities.

## 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)?*

IRS Information Technology (ROIU-RTS E-trak Developers/Administrators)

*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?*

Per the IT point-of-contact, the audit trail will collect the following information: user log-in information; created and deleted activities; log-out details; the information collected on who performed the activities.

## 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: Under 5,000

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