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: February 11, 2015 PIA ID Number: **1157**

1. What type of system is this? e-trak ROIU-RTS System, ROIU

2. Is this a new system? Yes

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

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

Next, enter the **date** of the most recent PIA.

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?

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
Yes	System Development/Milestone 4B
No	System Deployment/Milestone 5
No	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 ROIU e-trak system will provide a means for tracking and assigning TIGTA reports of investigation to business units within the IRS. It will also provide a reporting system to gather data. 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.

B. PII DETAIL

6. Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information, 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 variations of SSN s (i.e. last 4 digits, etc.)? Yes

If **yes**, check who the SSN (or SSN variation) is collected on.

Yes	On Primary	No	On Spouse	No	On Dependent

If **yes**, check all types SSN s (or variations of SSN s) 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)
Yes	Preparer Taxpayer Identification Number (PTIN)

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

We do not track reports of investigation by the SSN or any other tax identification number. However, complaint documents might contain this information. We do not input SSNs into the e-trak application.

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

If **yes**, specify the information.

Selected	PII Element	On Primary	On Spouse	On Dependent
Yes	Name	Yes	Yes	Yes
Yes	Mailing address	No	No	No
Yes	Phone Numbers	No	No	No
Yes	E-mail Address	No	No	No
Yes	Date of Birth	Yes	Yes	Yes
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
Yes	Criminal History	No	No	No
Yes	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
Yes	Financial Account Numbers	No	No	No
No	Photographic Identifiers	No	No	No
No	Biometric Identifiers	No	No	No
Yes	Employment (HR) Information	No	No	No
Yes	Tax Account Information	Yes	Yes	Yes
No	Live Tax Data	No	No	No

6c. Does this system contain SBU information the system that it uses, collects, receives, displays, stores, maintains, or disseminates? Yes

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

Selected	SBU Name	SBU Description
Yes	Agency Sensitive Information	Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission
Yes	Procurement sensitive data	Contract proposals, bids, etc.
Yes	Official Use Only (OUO) or Letter of Understanding (LOU)	Documents that have been marked OUO or LOU
Yes	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
Yes	Physical Security Information	Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities
Yes	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
Yes	SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
Yes	PII for personnel administration is 5 USC
No	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

If the answer to 6f is **No**, verify the authority is correct with the system owner and then update the answer to 6f.

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 variations) are used, explicitly explain why use of SSNs meets this criteria. Be specific.

We WILL NOT USE SBU/PII INFORMATION TO TRACK REPORTS OF INVESTIGATION IN THE E-TRAK SYSTEM. However, we will store this information as we receive it from the TIGTA in the same manner that we store this information for TIGTA complaint referrals in the ECCO e-trak system. We will not refer TIGTA ROIs concerning employee misconduct through this e-trak system. We have a separate process to forward the employee misconduct ROIs to the servicing LR offices. However, we will refer NON-EMPLOYEE reports of investigation to the appropriate business units through his new ROIU e-trak system.

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.

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.

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? No

D. RESPONSIBLE PARTIES

N/A

E. INCOMING PII INTERFACES

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

11a. If **yes**, does the system receive SBU/PII from IRS files and databases?

No System Records found.

11b. Does the system receive SBU/PII from other federal agency or agencies?

No Organization Records found.

11c. Does the system receive SBU/PII from State or local agency (-ies)?

No Organization Records found.

11d. Does the system receive SBU/PII from other sources?

No Organization Records found.

11e. Does the system receive SBU/PII from **Taxpayer** forms?

No Tax Form Records found.

11f. Does the system receive SBU/PII from **Employee** forms (such as the I-9)?

No Employee Form Records found.

F. PII SENT TO EXTERNAL ORGANIZATIONS

12. Does this system disseminate SBU/PII? Yes

12a. Does this system disseminate SBU/PII to other IRS Systems? No

No System Records found.

12b. Does this system disseminate SBU/PII to other Federal agencies? No

No Organization Records found.

12c. Does this system disseminate SBU/PII to State and local agencies? No

No Organization Records found.

12d. Does this system disseminate SBU/PII to IRS or Treasury contractors? No

No Organization Records found.

12e. Does this system disseminate SBU/PII to other Sources? No

No Organization Records found.

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

17a. If **yes**, how is notice provided? Was the individual notified about the authority to collect the information, whether such is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects, if any, if they decide not to provide any of the requested information?

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.
We do not collect the SBU/PII information. That is the role and responsibility of the TIGTA.

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

If no, why not? Again, we do not collect the SBU/PII information. The TIGTA collects the information and forwards it to the IRS in the complaint or allegation.

19. 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. We share the information within the agency, only on a need-to-know basis. This is a FISMA reportable system.

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 and Write
Sys. Administrators	Yes	Administrator
Developers	Yes	Read-Only

Contractor Employees? No

21a. 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.

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

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.

The etrak ROIU-RTS is unscheduled. A SF-115 request for records disposition authority for eTrak ROIU-RTS data and associated records will be drafted with the assistance of the IRS Records and Information Management (RIM) Program Office, and submitted to the National Archives and Records Administration (NARA) for disposition approvals. HCO is likely to propose a 3-year disposition that mirrors the IT Division's records retention for eTrak records.

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)? In-process

If **in process**, when is the anticipated date of the SA&A or ECM-R completion? 4/20/2015 12:00:00 AM

23.1 Describe in detail 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.

I.2 SA&A OR ECM-R

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

If **yes**, Is the test plan in process or completed: In Process

If **in process**, when is the test plan scheduled for completion? 6/15/2015 12:00:00 AM

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?

Per the IT point-of-contact, the System Test Plan describes the approach that the e-trak ROIU-RTS system deliverable work product will tested to meet system's functions and specifications, including the Privacy requirements. The System Test Plan is developed in accordance with the procedures in Internal Revenue Manual (IRM) 2.127 Software Testing Standards and Procedures. The testing activities are being conducted on the e-trak ROIU-RTS system to validate each of the Privacy requirements are as follows: Strict Confidentiality: Generate test cases with instructions to valid users and non-valid users and ensure the PII protection where only authorized users allowed access to the system. Test Script will be used to verify Access control is managed through the OL5081 system is protected from non-authorized users Accountability: Generate test cases to verify the assigned user roles (i.e. Administrator Role, ROI Specialist, BU Specialist, etc...) have the designated and appropriate permissions. The testing will be performed to determine the type of actions performed, when actions were performed, and by whom. Security: Security Testing and evaluation is conducted on all of the e-trak ROIU-RTS system following the IRS security guidelines. This system is a FISMA reportable system and currently e-trak is conducting the annual FISMA security control assessment and providing evidence to satisfy the Privacy requirements Privacy Awareness and Training: e-trak has a plan in place to review and validate training completion by requesting completion certificates from all system users. Purpose Limitation: N/A. The PII purpose is limited to being stored in attached documents. The system does not collect nor process the PII data. Create a test case – ensure that none of the system fields allow the entry of PII data. Minimization of collection, use, retention, disclosure: The e-trak ROIU-RTS system will have test script that outlines the precise steps to ensure PII information is only stored in documents attached to a case and nowhere else. The PII retention will follow Information Technology procedures under IRM 1.15.6. The retention and disclosure of personally identifiable information will be limited to what is minimally necessary for the specific purposes in the e-trak ROIU-RTS system.

K. LIVE DATA TESTING

25. Does this system use, or plan to use Live 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

If **other**, identify the category of records and the number of corresponding records (to the nearest 10,000).

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

If **yes**, provide a citation and/or link to the most recent Treasury data-mining report to Congress in which your system was discussed (if applicable).

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

If **yes**, describe the type of information derived from these efforts and the technical (e.g., audit trails) or other processes used to limit unauthorized monitoring.

N. ACCOUNTING OF DISCLOSURES

30. Does the system include or require disclosure of tax or employee information to anyone other than IRS employees or IRS contractors 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

If **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.

30a**.** If **no**, accounting of Disclosures risk noted. Contact *Disclosure* to develop an accounting of disclosures. Explain steps taken to develop accounting of disclosures process.

30b. If **N/A**, explain the Exemption and/or Disclosure s response.

End of Report