Date of Approval: January 19, 2018 PIA ID Number: **3136**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. ETRAK ROI UNIT REPORT AND TRACKING SYSTEM, ROIU-RTS SYSTEM

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.

ETRAK ROI UNIT REPORT AND TRACKING SYSTEM, ROIU-RTS SYSTEM, 1157

Next, enter the **date** of the most recent PIA. 2/11/2015

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

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 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.

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	No	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)
Yes	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).

We do not track reports of investigations by the SSN's or any other tax identification number. However, the Report of Investigation Unit (ROIU) does scan in Report of Investigations cases and those reports do have PII information contained within them, (i.e. Subject Name, Place of Birth, Date of Birth, Physical Description of Subject, Gender, Social Security Number, Criminal Rap Sheet). The Office of Management and Budget memorandum M-07-12 requires that federal agencies develop a mitigation or elimination strategy for systems that uses SSN's, 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 Report of Investigation Unit e-trak program requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer at this time. SSN's are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayer 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	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	No	No
No	Place of Birth	No	No	No
Yes	SEID	No	No	No
Yes	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
Yes	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
Yes	Employment (HR) Information	No	No	No
Yes	Tax Account Information	Yes	No	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
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 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.
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

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 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).

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

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.

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/IRS 00.001	Correspondence

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. ## For Official Use Only

E. INCOMING PII INTERFACES

11. Does the system receive SBU/PII from other system or agencies? Yes

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

If **yes**, enter the files and databases.

System Name	Current PIA?	PIA Approval Date	SA & A?	Authorization Date
ALERTS (Automated Labor & Employee Relations Tracking System)	Yes	02/24/2017	Yes	02/06/2017
TIMIS (Time Management Information System)	Yes	05/01/2015	No	02/06/2017

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

If **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).

Organization Name	Transmission method	ISA/MOU
Office of Personnel Management	MAIL	Yes

11c. Does the system receive SBU/PII from State or local agency (-ies)? No

11d. Does the system receive SBU/PII from other sources? No

11e. Does the system receive SBU/PII from **Taxpayer** forms? No

11f. Does the system receive SBU/PII from **Employee** forms (such as the I-9)? No

If **yes**, identify the forms

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, 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.
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.

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? 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.

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. 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.

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. 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.

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?

Yes

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? Yes

22a. If **yes**, how long are the records required to be held under the corresponding RCS and how are they disposed of? In your response, please include the complete IRM number 1.15.XX and specific item number and 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) 1, Item 3, and as coordinated with the IRS Records and Information Management (RIM) Program and IRS Records Officer.

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? 2/11/2015

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.

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?
Per the IT point-of-contact, the System Test Plan describes the approach that the e-trak ROIU-RTS system deliverable work product will be 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.

24b.1. If **completed**, where are the test results stored (or documentation that validation has occurred confirming that requirements 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 be 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.

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