

Date of Approval: 01/03/2025  
Questionnaire Number: 1844

## Basic Information/Executive Summary

What is the name of your project (system, database, pilot, product, survey, social media site, etc.)?

e-Trak Whistleblower

Acronym:

eTrakWB

Business Unit

Whistleblower Office

Preparer

# For Official Use Only

Subject Matter Expert

# For Official Use Only

Program Manager

# For Official Use Only

Designated Executive Representative

# For Official Use Only

Executive Sponsor

# For Official Use Only

Executive Summary: Provide a clear and concise description of your project and how it will allow the IRS to achieve its mission.

This system collects limited information on the investigation of the alleged tax violations made by the claimants, including a scanned attachment of the Form 211 which contains the allegations and the whistleblowers estimate of the tax type, years, and amounts of the potential violation. Tax cases setup for investigation, litigation or prosecution based on the information received, will be handled in the appropriate Business Division following the Internal Revenue Code (IRC) procedures mandated by law.

# Personally Identifiable Information (PII)

Will this project use, collect, receive, display, store, maintain, or disseminate any type of Sensitive but Unclassified (SBU), Personally Identifiable Information (PII), or Federal Tax Information (FTI)?

Yes

Please explain in detail how this project uses sensitive data from inception to destruction (data lifecycle).

The e-Trak Whistleblower system requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer at this time. We collect the SSN (Social Security Number)/EIN (Employer Identification Number)/TIN (Taxpayer Identification Number) to ensure we are awarding the correct taxpayer and issuing Form 1099 for award recipients.

Please select all types of Sensitive but Unclassified data (SBU)/Personally Identifiable Information (PII)/Federal Tax Information (FTI) that this project uses.

Address

Email Address

Individual Taxpayer Identification Number (ITIN)

Social Security Number (including masked or last four digits)

Tax ID Number

Telephone Numbers

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

PII for federal tax administration - generally IRC Sections 6001 6011 or 6012

SSN for tax returns and return information - IRC section 6109

# Product Information (Questions)

1.1 Is this PCLIA a result of the Inflation Reduction Act (IRA)?

No

1.3 What type of project is this (system, project, application, database, pilot/proof of concept, power platform/visualization tool)?

System

1.35 Is there a data dictionary for this system?

Yes

1.36 Explain in detail how PII and SBU data flow into, through and out of this system.

We collect this information for use in determining the correct amount of any award payable to you under 26 USC 7623. We may disclose this information as authorized by 26 USC 6103, including to the subject taxpayer(s) as needed in a tax compliance investigation and to the Department of Justice for civil and criminal litigation. You are not required to apply for an award. However, if you apply for an award, you must provide as much of the requested information as possible. Failure to provide information may delay or prevent processing your request for an award; providing false information may subject you to penalties. eTrakWB users (IRS employees) collect PII/SBU data based on Taxpayer forms (Form 211 and Form 3949) and manually enter eTrakWB system. We will issue letter and Form 1099 for award recipients.

1.4 Is this a new system?

no

1.5 Is there a Privacy and Civil Liberties Impact Assessment (PCLIA) for this system?

yes

1.6 What is the PCLIA number?

8245

1.7 What are the changes and why?

Recently e-Trak has completed the FISMA25 Annual Security Controls Assessment (ASCA). Based on the risk assessment result, Privacy Compliance & Assurance team (PCAT) has identified a security control finding against e-Trak. This weakness finding is related to Privacy Impact Assessments (RA-8) due to the failure to maintain an accurate answer to Q12 and 12.a on PCLIA #8245. This finding is impacted to eTrakWB that has PII/FTI captured/stored/disseminate to other system, and audit trail data log is being sent to SPLUNK Enterprise Security. To mitigate this privacy risk, a new PCLIA (#1844) is required and created in PIAM.

1.8 If the system is on the As-Built-Architecture (ABA), what is the ABA ID number of the system? If this PCLIA covers multiple applications shown on the ABA, please indicate the ABA ID number(s) for each application covered separated by a comma. If the system is not in the ABA, then contact the ABA (<https://ea.web.irs.gov/aba/index.html>) for assistance.

211503

1.9 What OneSDLC State is the system in (Allocation, Readiness, Execution)?

Execution

2.1 If this system discloses any PII to any third party outside the IRS, 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. Enter "Yes" or "No". If Exempt, type "Exempt".

No

2.2 Please provide the full name of and acronym of the governance board or Executive Steering Committee (ESC) this system reports to.

Application Development (AD) Compliance.

3.1 Does your project/system involve any use of artificial intelligence (AI), including virtual assistant, chat bot, and robotic process automation, as defined in Executive Order 13960?

No

3.3 Does this system use cloud computing?

No

3.6 Does this system interact with the public through a web interface?

No

3.7 Describe the business process allowing an individual to access or correct their information.

All the process and procedures are dictated by the Internal Revenue Manual guidelines. IRS policy allows individuals whose data is in the system the opportunity to clarify or dispute negative determinations through the appeals process.

4.1 Who owns and operates the system (IRS Owned and Operated, IRS Owned and Contractor Operated, Contractor Owned and Operated)?

IRS Owned and Operated.

4.2 If a contractor owns or operates the system, does the contractor use subcontractors?

No

4.5 Identify the roles and their access level to the PII data. For contractors, indicate whether their background investigation is complete or not.

For IRS Employees: Users: Read and Write Access Managers: Read and Write Access Sys. Administrators Read and Write Access Developers: No Access for Contractors: No contractors and No Access

4.51 How many records in the system are attributable to IRS Employees? Enter "Under 50,000", "50,000 to 100,000", "More than 100,000" or "Not Applicable".

Not Applicable

4.52 How many records in the system are attributable to contractors? Enter "Under 5,000", "5,000 to 10,000", "More than 10,000" or "Not Applicable".

Not Applicable

4.53 How many records in the system are attributable to members of the public? Enter "Under 100,000", "100,000 to 1,000,000", "More than 1,000,000" or "Not applicable".

100,000 to 1,000,00.

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

Permission for access to the data is determined by the Whistleblower Application System Administrator in the Whistleblower Office with the concurrence of the Director of the Whistleblower Office or his delegate. Access is removed when the IRS employee no longer has need to access the system. Data access is granted on a need-to-know basis. A potential user must submit a request for access via Business Entitlement Access Request System (BEARS) to their local management for approval consideration. Users are not permitted access without a signed BEARS form from an authorized management official. Specific permissions (Read, Write, Modify, Delete, and/or Print) are defined on the BEARS 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.

5.1 Please describe any privacy risks, civil liberties and/or security risks identified for the system that need to be resolved and what is the mitigation plan?

Only 1 privacy risk has been identified to correct the questionnaire (Q12 and 12.a on PCLIA #8245) about disseminate PII (audit trail data log) to SPLUNK. Audit trail data log is available for SPLUNK to retrieve. The mitigation plan is to submit a new PCLIA #1844 to update the PCLIA questionnaire. In addition, open a POAM (Plan of Action and Milestone) in AARG (Assessment, Authorization, and Risk Governance) to address and resolve the finding.

5.11 Is there a Risk Assessment Form and Tool (RAFT) associated with this system on file with your organization or the IRS Risk Office.

No

5.2 Does this system use or plan to use SBU data in a non-production environment?

No

## Interfaces

### Interface Type

IRS Systems, file, or database

Agency Name  
SPLUNK  
Incoming/Outgoing  
Outgoing (Sending)  
Transfer Method  
Other  
Other Transfer Method  
SPLUNK Universal Forwarder

**Interface Type**

Forms  
Agency Name  
Form 3949 - Information Report Referral  
Incoming/Outgoing  
Incoming (Receiving)  
Transfer Method  
Mail

**Interface Type**

Forms  
Agency Name  
Form 211- Application for Award for Original Information  
Incoming/Outgoing  
Incoming (Receiving)  
Transfer Method  
Mail

## **Systems of Records Notices (SORNs)**

**SORN Number & Name**

IRS 42.005 - Whistleblower Office Records  
Describe the IRS use and relevance of this SORN.  
IRS is required to have a published Privacy Act system of records in the Federal Register. The records in this system will be used to administer the claimant award program under 26 U.S.C. 7623.

**SORN Number & Name**

IRS 34.037 - Audit Trail and Security Records  
Describe the IRS use and relevance of this SORN.  
To meet the enterprise audit trail requirement. To identify and track any unauthorized accesses to sensitive but unclassified information and potential breaches or unauthorized disclosures of

such information or inappropriate use of government computers to access Internet sites for any purpose forbidden by IRS policy

## Records Retention

What is the Record Schedule System?

Record Control Schedule (RCS)

What is the retention series title?

Administrative and Organizational Records

What is the GRS/RCS Item Number?

(RCS) 8, item 37.

What type of Records is this for?

Both (Paper and Electronic)

Please provide a brief description of the chosen GRS or RCS item.

The Whistleblower software application includes information collected and maintained by, or at the direction of the IRS Whistleblower Office, to determine claimants' eligibility for awards under 26 U.S.C. 7323. Whistleblower System data is approved for destruction 6 years, 3 months after the fiscal year in which it was created in accordance with National Archives-approved Job No. N1-58-09-52. These disposition instructions are published in IRS Document 12990 under Records Control Schedule (RCS) 8, item 37. These instructions are in concert with records requirements for Informant Claims in Section 6501(c)(2).

What is the disposition schedule?

(A) Inputs: The Whistleblower Application receives inputs manually from various sources including correspondence, memoranda, e-mail, telephone contacts, and staff notes  
AUTHORIZED DISPOSITION Not Applicable. The official records of all inputs are appropriately scheduled under various items in Records Control Schedules 8, 15, 33 and 43. (B) System Data: Contents of the Whistleblower Application include, but are not limited to, the following: name or other identifying number for the whistleblower, address and telephone number of the whistleblower, status of the investigation, status of payment, payment amount, and payment date. (Job No. N1-58-09-52)  
AUTHORIZED DISPOSITION Cut off files at the end of the fiscal year. Destroy 6 years and 3 months after cutoff. Note: Payments to IRS whistleblowers are subject to audit by the General Accountability Office (GAO). (C) Outputs: Outputs from the Whistleblower Application include a variety of reports. Documentation generated from eTrak-supported applications including the Whistleblower Application consist of weekly and/or biweekly reports of activities, status, trends, and statistics.

Documentation also provides reports to the current status of  
Servicewide actions/activities. (GRS 5.2, Item 020; Job No. DAA-  
GRS-2017-0003-0002) AUTHORIZED DISPOSITION  
Destroy/Delete when obsolete or no longer needed.