

Whistleblower Office Records System (e-trak Whistleblower) – Privacy Impact Assessment

PIA Approval Date – May 12, 2011

System Overview

The Whistleblower Records system includes information collected and maintained by, or at the direction of, the IRS Whistleblower Office, to determine claimants' eligibility for awards under 26 USC 7623. This system collects limited information on the investigation of the alleged tax violations made by the claimants. 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.

System of Records Notice (SORN):

- IRS 42.002--Whistleblower Records
- IRS 34.037--IRS Audit Trail and Security Records system

Data in the System

1. Describe the information (data elements and fields) available in the system in the following categories:

- A. Taxpayer –Taxpayer's Name, Social Security Number (SSN) or Employer Identification Number (EIN) and Address
- B. Employee – The system contains the name of the employee and Standard Employee Identification (SEID) of the employee assigned the case.
- C. Audit Trail – The system contains the SEID of the employee and date that the case was accessed.
- D. Other –These records include information about individuals of possible tax noncompliance and claims for award to the Whistleblower Office. Records are kept by the name of the representative and informant.

2. Describe/identify which data elements are obtained from files, databases, individuals, or any other sources.

- A. IRS – Information may be obtained from the Operating Divisions or Criminal Investigations on a need to know basis.
- B. Taxpayer –Information is not obtained directly from the taxpayer.
- C. Employee – Only IRS employees with a need to know may access a case.
- D. Other Third Party Sources – Information is obtained from an Informant and/or the informant's representative.

3. Is each data item required for the business purpose of the system? Explain.

Each data item is required to track the disposition of the informant's claim.

4. How will each data item be verified for accuracy, timeliness, and completeness?

The staff of the Whistleblower Office verifies each data element for accuracy, timeliness and completeness based on the information received by the Whistleblower, or their representative.

5. Is there another source for the data? Explain how that source is or is not used.

No.

6. Generally, how will data be retrieved by the user?

Data may be retrieved by name of the informant or case number.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?

Yes, as stated above, by informant name or case number, and only by authorized personnel who have approved access to the system.

Access to the Data

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?

When the Whistleblower Office determines who needs access, staff, Revenue Agents and Counsel Attorneys will be granted access to the data by submitting a Form 5081.

Note: Contractors do not have access to the application.

9. How is access to the data by a user 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.

10. Do other IRS systems provide, receive, or share data in the system?

No.

11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?

Not applicable.

12. Will other agencies provide, receive, or share data in any form with this system?

No.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?

The data is purged following the requirements for Informant Claims in Section 6501(c)(2).

14. Will this system use technology in a new way?

No.

15. Will this system be used to identify or locate individuals or groups? If so, describe the business purpose for this capability.

No.

16. Will this system provide the capability to monitor individuals or groups? If yes, describe the business purpose for this capability and the controls established to prevent unauthorized monitoring.

No.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?

No.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?

Not applicable.

19. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors?

No.

[View other PIAs on IRS.gov](#)