Date of Approval: **December 14, 2022**

PIA ID Number: **7450**

SYSTEM DESCRIPTION

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

e-Trak Whistleblower, etrak-wb

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?

e-Trak Whistleblower, etrak-wb PIA 4684

What is the approval date of the most recent PCLIA?

3/11/2020

Changes that occurred to require this update:

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.

Application Development (AD) Compliance.

Current ELC (Enterprise Life Cycle) Milestones:

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 IRS Whistleblower Office was created by Section 406 of the Tax Relief and Health Care Act of 2006. Section 406 addresses "whistleblowers" who provide information on significant non-compliance with tax laws and the awards allowed to them under 26 USC 7623. In the past, within the Service, this program was referred to as the "informants program." The amendment also establishes award percentage ranges for cases in which more than $2 million in tax, penalties and interest are in dispute, and requires that award determinations in those cases be made by the Whistleblower Office. 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, 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.

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:

Another compelling reason for collecting the SSN

Explain why the authorized use(s) above support the new or continued use of SSNs (or tax identification numbers).

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/EIN/TIN to ensure we are awarding the correct taxpayer and issuing Form 1099 for award recipients.

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

The Office of Management and Budget memorandum circular A-130 requires that federal agencies develop a mitigation or elimination strategy for systems that use SSNs, 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 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. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns.

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
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.

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

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.

We collect the SSN/EIN/TIN to ensure we are awarding the correct taxpayer and issuing form1099 for award recipients. Addresses, phone numbers and emails are used to send forms for signatures and to communicate with taxpayers for additional information.

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

The data is collected directly from the individual for whom it relates. The information is manually verified with the individual prior to settlement of the award claim and an opportunity to correct the information is provided at that time. The system does not interact with nor receive information from any other IRS system.

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 42.005 Whistleblower Office Records

IRS 34.037 Audit Trail and Security Records

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?

No

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?

Yes

Please identify the form number and name:

Form Number: Form 211
Form Name: Application for Award For Original Information

Form Number: Form 3949
Form Name: Information Report Referral

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?

Yes

How is notice provided? Was the individual notified about the authority to collect the information, whether disclosure is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects on the individual, if any, if they decide not to provide all or any of the requested information?

Privacy Act statement on Form 211, Application for Award for Original Information, which provides the information collected. Privacy Act statement is as follows: We ask for the information on this form to carry out the internal revenue laws of the United States. Our authority to ask for this information is 26 USC 6109 and 7623. 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.

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

Yes

Describe the mechanism by which individuals indicate their consent choice(s):

By submitting a completed Form 211, Application for Award for Original Information, they consent to provide the information. The Privacy Act statement incorporates a statement: "...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." The information only needs to be provided if they are applying for an award.

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

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.

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: Read Write

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.

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.

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). RCS 8 Item 37(a)-Whistleblower Application-Disposition Not Applicable. The official records of all inputs are appropriately scheduled under various items in Records Control Schedules 8, 15, 33 and 43. RCS 8 Item 37(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.-Destroy/Delete 6 years and 3 months after cutoff. RCS 8 Item 37(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.-Destroy/Delete when obsolete or no longer needed. RCS 8 Item 37(d)-Documentation: System documentation for the Whistleblower Application consists of eTrak codebooks, records layout, user guide, and other related materials.-Destroy/Delete when superseded or 5 years after the application is terminated, whichever is sooner.

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?

10/25/2022

Describe the system's audit trail.

All account access to the system is granted through the BEARS authorization process thus ensuring that authorization is granted from appropriate designated officials and that identifiers are securely distributed to the individuals requesting access. E-trak regularly runs audits to determine accounts that no longer need access to PII or need to be inactive. Per IRM 10.8.1.5.1.3, after 120 days of inactivity, the user's account will be disabled, but not removed from the system. After 365 days of inactivity, the account will be automatically deleted. Disabled or deleted accounts require that the user go through the BEARS process to regain access to the system. In addition, the SSP is reviewed annually during continuous monitoring initiatives, and updated at least every three years or whenever there are significant changes to the system.

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)?

The test cases, test scripts and test plans are generated and stored in Collaborate Lifecycle Management Quality Manager Tool.

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?

Continuous Monitoring (eCM) (now called Annual Security Control Assessment (ASCA)) occurs annually to ensure that controls remain in place to properly safeguard PII. This process creates test cases and test scripts for security and privacy requirements. These test cases and test scripts are to validate and verify user access control procedures, ensure strict confidentiality, use of data, and accountability. In addition, e-Trak system is currently in the Operations and Maintenance phase of its lifecycle. Continuous Monitoring (eCM) (now called Annual Security Control Assessment) occurs annually to ensure that controls remain in place to properly safeguard PII.

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: Not Applicable

Contractors: Not Applicable

Members of the Public: 100,000 to 1,000,000

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