Date of Approval: **February 20, 2020**

PIA ID Number: **4646**

SYSTEM DESCRIPTION

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

e-Trak EPS, e-Trak EPS

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 Employee Protection System (EPS), e-Trak EPS 3564

What is the approval date of the most recent PCLIA?

8/27/2018

Changes that occurred to require this update:

Addition of Personally Identifiable Information (PII)

Were there other system changes not listed above?

Yes

What were those changes?

EPS is altering the System of Records Notice (SORN) for Office of Employee Protection based on new criteria. The categories of the individuals covered by EPS e-Trak is changing to include adding language to include "former" IRS employees when the action/behavior relates to their official duties, as this behavior has a nexus to how individuals might behave toward current employees performing tax administration activities. Also, the "active" qualifier, as it applies to membership in group(s) advocating violence, was removed since it is difficult to measure and does not bolster the categorization. Membership in group(s) advocating violence is sufficient to pose a threat that needs consideration when planning for taxpayer interactions.

In addition, due to the current landscape of self-radicalization, a new criterion was added to include persons who are known to advocate violence against IRS employees without known membership in the aforementioned groups/organizations. The altered SORN also adds a 10-year look-back period to existing criteria and the new proposed criterion regarding persons who are known to advocate violence against IRS employees without known membership in any related groups/organizations to ensure the IRS considers actions/behaviors that might provide insight into potential threats thus allowing IRS staff to react accordingly. The new look-back period sets clear time frames and removes the current vague, open-ended language for criteria one through four. Additionally, the proposed change of the look-back period from five years to 10 years for criterion five, regarding individuals who have demonstrated a clear propensity toward violence through act(s) of violent behavior, helps protect IRS staff against potential threats. For example, this allows consideration for Individuals who may have been incarcerated in the past five years but were convicted of violent acts that occurred within the past 10 years.

What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym.

Privacy, Governmental Liaison & Disclosure (PGLD) Governance Board

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 purpose of EPS is to catalogue information and data about Potentially Dangerous Taxpayer (PDT) and Caution Upon Contact (CAU) taxpayer cases. These cases identify taxpayers who represent a potential danger to the Internal Revenue Service (IRS) and/or IRS Employees, and include information as to why the taxpayer is considered a potential danger. EPS was developed in-house in 2003 using Informix, and it was converted to Oracle in 2009. EPS is a moderate risk application containing Sensitive but Unclassified (SBU) data and Personally Identifiable Information (PII), including information about the taxpayer, the nature of the incident, and the employee who reported the incident. The PII that is collected includes the taxpayer's name, address, date of birth (DOB), social security number (SSN), and employer identification number (EIN), if applicable. The EPS database receives information daily from the Treasury Inspector General for Tax Administration (TIGTA). While the information in EPS is important to all IRS employees with public contact, the data

is only accessible to authorized Office of Employee Protection (OEP) users who require access to perform their respective jobs. Limited access may be granted to the Government Accounting Office (GAO) or TIGTA for auditing purposes. In these instances, the access rights are temporary and read-only.

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:

When there is no reasonable alternative means for meeting business requirements

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

The e-Trak EPS system requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include SSNs on their income tax returns.

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 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. e-Trak EPS requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer at this time.

Employer 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

Date of Birth

Criminal History

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

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.

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

Criminal Investigation Information Information concerning IRS criminal investigations or the agents conducting the investigations.

Are there other types of SBU/PII used in the system?

Yes

Describe the other types of SBU/PII that are applicable to this system.

If the taxpayer is designated as a PDT criterion #4, the narrative would likely state that taxpayer was arrested for assault on a police officer.

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

PII for personnel administration is 5 USC

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.

The primary purpose is for the protection of IRS employees from potentially dangerous taxpayers and taxpayers who should be approached with caution. There is no plan to eliminate the use of SSNs in this system, due to the fact that the entire purpose of the system is linked to the taxpayer's SSN. Without the SSN, there would be no ability to input the PDT/CAU indicators into Integrated Data Retrieval System (IDRS) or ensure that only warranted indicators are reflected on IDRS.

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

Once information is received from TIGTA, it is crossed-referenced with IDRS. OEP also performs a semi-annual review of Individual Master File (IMF) and Business Master File (BMF) and/or Non-Master File Reports against the EPS database to ensure that only warranted PDT and/or CAU indicators are reflected on Master File and/or Non-Master File accounts.

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 60.000 Employee Protection System 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?

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).

Name: TIGTA

Transmission Method: Electronic File Transfer Utility (EFTU)

ISA/MOU: 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?

No

Does the system receive SBU/PII from Employee forms (e.g. the I-9)?

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

Yes

Does this system disseminate SBU/PII to other IRS Systems?

No

Does this system disseminate SBU/PII to other Federal agencies?

No

Does this system disseminate SBU/PII to State and local agencies?

Yes

Identify the full names of the state and local agency(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name: Various State and Local agencies

Transmission Method: Secure Data Transfer (SDT)

ISA/MOU: Yes

Identify the authority

Inter-agency agreement (ISA)- Disclosure is authorized under an Internal Revenue Code section 6103(d).

Identify the Routine Use in the applicable SORN (or Privacy Act exception)

Disclosure of returns and return information may be made only as provided by 26 U.S.C. 6103.

For what purpose?

Potentially Dangerous Taxpayer (PDT) List: A list of taxpayers designated as PDT, whose addresses of record are within the state, will be provided semi-annually.

Does this system disseminate SBU/PII to IRS or Treasury contractors?

No

Does this system disseminate SBU/PII to other Sources?

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?

The information within e-Trak EPS comes from another IRS program (IDRS). This system provides the Privacy Act Notice to individuals. e-Trak EPS 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 via IDRS and their related tax forms instructions, and pursuant to 5 USC. The IRS has the legal right to ask for information per IRC sections 6001, 6011, and 6012(a), and their regulations. The regulations state that "taxpayers must file a return or statement with IRS for any tax they are liable for." Their response is mandatory under these sections.

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):

The information within e-Trak EPS comes from another IRS program (IDRS). This system provides the Privacy Act Notice to individuals. e-Trak EPS 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 via IDRS and their related tax forms instructions, and pursuant to 5 USC. The IRS has the legal right to ask for information per IRC sections 6001, 6011, and 6012(a), and their regulations. The regulations state that "taxpayers must file a return or statement with IRS for any tax they are liable for." Their response is mandatory under these sections.

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

The information within e-Trak EPS comes from another IRS program (IDRS). This system provides the Privacy Act Notice to individuals. e-Trak EPS 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 via IDRS and their related tax forms instructions, and pursuant to 5 USC. The IRS has the legal right to ask for information per IRC sections 6001, 6011, and 6012(a), and their regulations. The regulations state that "taxpayers must file a return or statement with IRS for any tax they are liable for." Their response is mandatory under these sections.

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

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

The Acting Chief, OEP determines who has access to the system. Only OEP employees with authorized access are granted access to the data. Online Form 5081 is required for all users.

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.

The National Archives and Records Administration (NARA) approved EPS data disposition instructions under Job No. N1-58-07-2 (approved 5/3/2007). Data is approved for deletion/destruction after PDT or CAU indicator is removed. The BU intends to maintain data stripped of personal identifiers offline for an additional 5 years, and then delete. EPS retention requirements (including inputs, outputs and system documentation) are published under Records Control Schedule (RCS) 28 for Tax Administration - Collection, item 145. A. Inputs: Includes daily EPS referrals from TIGTA via file transfer protocol (FTP) scripts and manual updates from investigative case files. Data includes taxpayer identification, case summary, status information, and pertinent dates. AUTHORIZED DISPOSITION Delete/Destroy after input verification into EPS master files. B. Master Files: Maintains data relevant to those taxpayers designated as either a Potentially Dangerous Taxpayer (PDT) or Caution Upon Contact taxpayer (CAU), including TIGTA investigation case file information, and reports regarding the status of those taxpayers. AUTHORIZED DISPOSITION Delete/Destroy after PDT or CAU indicator is removed. Maintain data stripped of personal identifiers offline for an additional 5 years, then delete. C. Outputs: Reports and ad hoc queries pertaining to demographic information, number and types of designations, profiles of potentially dangerous taxpayers, and other relevant trend and statistical data. AUTHORIZED DISPOSITION Delete/Destroy when superseded or no longer needed. D. System Documentation: Codebooks and user guide. AUTHORIZED DISPOSITION Delete/Destroy when superseded or obsolete.

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?

11/14/2017

Describe the system's audit trail.

Testing is conducted annually to ensure the selected controls are functioning correctly. When testing of a security control reveals that the control is not functioning as expected, the control deficiency is documented in the system's plan of action and milestones (POA&M). All test results are documented and reported to Business Unit (BU) Security Project Management Office (SPMO).

The security state of the application is then reported to the appropriate organizational officials annually as defined in Treasury Directives Policy (TDP) 85-01. e-Trak EPS is following the appropriate audit trail elements pursuant to current audit logging security standards.

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)?

Continuous monitoring (ECM) now called Annual Security Control Assessment (ASCA) occurs annually to ensure that controls remain in place to properly safeguard PII.

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.

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: Under 100,000

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?

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.

Yes