Date of Approval: August 27, 2018 PIA ID Number: **3564**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. e-Trak EPS, e-Trak EPS

2. Is this a new system? No

2.a. If **no**, is there a Privacy Civil Liberties Impact Assessment (PCLIA) for this system? Yes

If **yes**, enter the full name, acronym, and milestone of the most recent PCLIA.

e-Trak Employee Protection System, e-Trak EPS, O&M, 03/13/2012

Enter the approval **date** of the most recent PCLIA. 04/03/2015

If **yes** Indicate which of the following changes occurred to require this update (check all that apply).

No Addition of Personally Identifiable Information (PII) (PII is any information that is linked or linkable).
No Conversions
No Anonymous to Non-Anonymous
No Significant System Management Changes
Yes 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
No Expiring PCLIA

Were there other system changes not listed above? No

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

Privacy Government Liaison & Disclosure (PGLD) Governance Board.

3.a. Check the current Enterprise Life Cycle (ELC) 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
No System Development/Milestone 4B
No System Deployment/Milestone 5
Yes 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 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). The Criminal Results Management System (CRMS) application sends data via SFTP (Secure File Transfer Protocol) to the GSS (General Support System) - 24 server where EPS resides. The file that is sent by TIGTA contains information about the referral including the taxpayer's name, SSN, address, and the referring employee's name. An Information Security Agreement (ISA) is in place between TIGTA and the IRS entitled the Interconnection Security Agreement between Treasury Inspector General for Tax Administration (TIGTA) and Internal Revenue Service (IRS) In Support of Network Integration, dated June 23, 2008. The EPS application is administered by the Office of Employee Protection (OEP) employees. Specialists within OEP manually enter the remaining information contained in the EPS database, such as criteria met, assigned and closure dates, etc. The types of manual data are date closures, criteria met, assigned specialist, and notes. TIGTA sends a daily report containing this information from the CRMS database, though a secure interface, to EPS. The indicators inform IRS employees that a particular taxpayer may pose a threat to them or the agency. While the information in EPS is important to all IRS employees with public contact, the data is only accessible to authorized 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.

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

6.a. 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 all types of tax identification numbers (TIN) that apply to this system:

Yes	Social Security Number (SSN)
Yes	Employer Identification Number (EIN)
No	Other Taxpayer Identification Number

If SSNs apply, which of the following approved Treasury uses of the SSNs applies:

No	Security background investigations
No	Interfaces with external entities that require the SSN
No	Legal/statutory basis (e.g. where collection is expressly required by statute)
Yes	When there is no reasonable alternative means for meeting business requirements
No	Statistical and other research purposes
No	Delivery of governmental benefits, privileges, and services
No	Law enforcement and intelligence purposes
No	Another compelling reason for collecting the SSN

Explain why one or more of the eight authorized uses above support the new or continued use of SSNs.

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).

There are no current plans to eliminate the use of SSNs. The Office of Management and Budget memorandum M-17-12 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.

6.b. Does this system use, collect, receive, display, store, maintain, or disseminate other (non-SSN) PII (i.e. Names, addresses, etc.)? Yes

If **yes**, specify the information.

Selected	PII Element
Yes	Name
Yes	Mailing address
No	Phone Numbers
No	E-mail Address
Yes	Date of Birth
No	Place of Birth
No	Standard Employee Identifier (SEID)
No	Mother's Maiden Name
No	Protection Personal Identification Numbers (IP PIN)
No	Internet Protocol Address (IP Address)
Yes	Criminal History
No	Medical Information
No	Certificate or License Numbers
No	Vehicle Identifiers
No	Passport Number
No	Alien Number
No	Financial Account Numbers
No	Photographic Identifiers
No	Biometric Identifiers
No	Employment Information
Yes	Tax Account Information
No	Centralized Authorization File (CAF)

6.c. 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
No	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.
No	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
No	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.

6.d. Are there other types of SBU/PII used in the system? No

6.e. 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
No	SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
No	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

6.f. 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 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.

8. How is the SBU/PII verified for accuracy, timeliness, and completeness?

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.

C. 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.

9. 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

If **yes**, enter the SORN number(s) and the complete the name of the SORN(s).

SORNS Number	SORNS Name
IRS 60.000	Employee Protection System Records
IRS 34.037	Audit Trail and Security Records System

*IRS is required to have a published Privacy Act system of records in the Federal Register. Please identify the Privacy Act SORN(s) that cover these records. If you need additional assistance identifying the correct SORNs please email *Privacy.*

D. RESPONSIBLE PARTIES

10. Identify the individuals for the following system roles. ##Official Use Only

E. INCOMING PII INTERFACES

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

11.a. If **yes**, does the system receive SBU/PII from IRS files and databases? No

11.b. 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
TIGTA	Electronic File Transfer Utility (EFTU)	No

11.c. Does the system receive SBU/PII from State or local agencies? No

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

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

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

F. DISSEMINATION OF PII

12. Does this system disseminate SBU/PII? Yes

12.a. Does this system disseminate SBU/PII to other IRS Systems? No

12.b. Does this system disseminate SBU/PII to other Federal agencies? No

12.c. Does this system disseminate SBU/PII to State and local agencies? Yes

If **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	Transmission method	ISA/MOU
various State and Local	Secure Data Transfer (SDT)	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.

12.d. Does this system disseminate SBU/PII to IRS or Treasury contractors? No

12.e. Does this system disseminate SBU/PII to other Sources? 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, Radio Frequency Identification (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 (or is) notice provided to the individual prior to collection of information? No

17.b. 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.
The only collection of information obtained is for IRS information only for employee protection, which is not provided by the individual but is collected by another IRS program (IDRS).

18. Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information? No

18.b. If individuals do not have the opportunity to give consent, why not?
The file that is sent by TIGTA contains information about the referral including the taxpayer's name, SSN, address, and the referring employee's name. An Information Security Agreement (ISA) is in place between TIGTA and the IRS entitled the Interconnection Security Agreement between Treasury Inspector General for Tax Administration (TIGTA) and Internal Revenue Service (IRS) In Support of Network Integration, dated June 23, 2008. This system is exempt from 5 U.S.C. 552a(c)(3), (d)(1)-(4), (e)(1), (e)(4) (G)-(I) and (f) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(2).

19. How does the system or business process ensure due process regarding information access, correction and redress?
Due process is not applicable to the public in general as the system does not "use" the event information to interact with the tax paying public in any way. IRS employees and contractors using IRS email and web services may face disciplinary action for the misuse of SSNs. All IRS employees will be given the opportunity to defend their actions before a final determination is made. Contractor employees will be afforded any rights granted within the regulations that cover the specific contract they are working under.

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-Only
Sys. Administrators	No	
Developers	No	

Contractor Employees? No

21.a. How is access to SBU/PII determined and by whom? The 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.

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

22.a. 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.

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.

I.2 SA&A OR ASCA

23. Has the system been through Security Assessment and Authorization (SA&A) or Annual Security Control Assessment (ASCA)? Yes

23.a. If **yes**, what date was it completed? 11/14/2017

23.1. Describe in detail 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.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? Yes

24.a. If **yes**, if yes, was the test plan completed? Yes

24.a.1. If **yes**, where are test results stored (or documentation that validation has occurred confirming that requirements have been met)? Yes, in TFIMS (Treasure FISMA Inventory Management System).

24.a.2. If **yes**, were all the Privacy Requirements successfully tested? Yes

24.a.3. If **yes**, are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved? No

24.1. Describe what testing and validation activities which have been conducted or are in process to verify and validate that the applicable Privacy Requirements (listed in header) have been met? Annual Continuous Monitoring TableTop Exercise FISMA 2015.

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:

26.a. IRS Employees:	Not Applicable
26.b. Contractors:	Not Applicable
26.c. Members of the Public:	Under 100,000
26.d. 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 Recommendations of the 9/11 Commission 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

30. Does Computer matching occur? No

N. ACCOUNTING OF DISCLOSURES

31. 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

    31.a. 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

End of Report