

NOTE: The following reflects the information entered in the PIAMS website.

A. SYSTEM DESCRIPTION

Authority: Office of Management Budget (OMB) Memorandum (M) 03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 & PVR #10- Privacy Accountability and #21-Privacy Risk Management

Date of Approval: April 3, 2015

PIA ID Number: **1327**

1. What type of system is this? Employee Protection System, EPS

2. Is this a new system? No

2a. If **no**, is there a PIA for this system? Yes

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

Employee Protection System, EPS

Next, enter the **date** of the most recent PIA. 3/13/2012 12:00:00 AM

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

No Addition of PII
No Conversions
No Anonymous to Non-Anonymous
Yes Significant System Management Changes
No 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

Were there other system changes not listed above? No

3. Check the current ELC (Enterprise Life Cycle) 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 Performance and Results Information System (PARIS) application sends data via SFTP to the GSS-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 Performance and Results Information System (PARIS) 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. EPS does not provide, send, or share data with any other IRS system.

B. PII DETAIL

6. Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information, any type of Sensitive but Unclassified (SBU) or Personally Identifiable Information (PII)? Yes

- 6a. If **yes**, does the system use, collect, receive, display, store, maintain, or disseminate Social Security Numbers (SSN s) or variations of SSN s (i.e. last 4 digits, etc.)? Yes

If **yes**, check who the SSN (or SSN variation) is collected on.

Yes On Primary Yes On Spouse No On Dependent

If **yes**, check all types SSN s (or variations of SSN s) that apply to this system:

Yes Social Security Number (SSN)
Yes Employer Identification Number (EIN)
Yes Individual Taxpayer Identification Number (ITIN)
No Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
No Preparer Taxpayer Identification Number (PTIN)

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

Not applicable due to system purpose.

6b. Does this system contain other (non-SSN) PII that it uses, collects, receives, displays, stores, maintains, or disseminates according to Privacy Requirements? (i.e. Names, addresses, etc.) Yes

If **yes**, specify the information.

<u>Selected</u>	<u>PII Element</u>	<u>On Primary</u>	<u>On Spouse</u>	<u>On Dependent</u>
Yes	Name	Yes	Yes	No
Yes	Mailing address	No	No	No
No	Phone Numbers	No	No	No
No	E-mail Address	No	No	No
Yes	Date of Birth	Yes	No	No
No	Place of Birth	No	No	No
No	SEID	No	No	No
No	Mother's Maiden Name	No	No	No
No	Protection Personal Identification Numbers (IP PIN)	No	No	No
No	Internet Protocol Address (IP Address)	No	No	No
Yes	Criminal History	No	No	No
No	Medical Information	No	No	No
No	Certificate or License Numbers	No	No	No
No	Vehicle Identifiers	No	No	No
No	Passport Number	No	No	No
No	Alien (A-) Number	No	No	No
No	Financial Account Numbers	No	No	No
No	Photographic Identifiers	No	No	No
No	Biometric Identifiers	No	No	No
No	Employment (HR) Information	No	No	No
No	Tax Account Information	No	No	No
No	Live Tax Data	No	No	No

6c. Does this system contain SBU information the system that it uses, collects, receives, displays, stores, maintains, or disseminates? Yes

If **yes**, select the types of SBU

<u>Selected</u>	<u>SBU Name</u>	<u>SBU Description</u>
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	Documents that have been marked OOU or LOU

	(OUO) or Letter of Understanding (LOU)	
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.

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

6e. Cite the authority for collecting SBU/PII (including SSN if relevant)

<u>Yes</u>	PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)
<u>No</u>	SSN for tax returns and return information is Internal Revenue Code Section 6109
<u>No</u>	SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
<u>No</u>	PII for personnel administration is 5 USC
<u>No</u>	PII about individuals for Bank Secrecy Act compliance 31 USC
<u>No</u>	Information by CI for certain money laundering cases may be 18 USC

6f. 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 variations) 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 IDRS or ensure that only warranted indicators are reflected on IDRS.

8. How is the SBU/PII verified for accuracy, timeliness, and completeness? Explain how steps are taken to ensure that all information maintained by the system that is used by IRS to make any adverse determination about an individual's rights, benefits, and/or privileges is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination.

Once information is received from TIGTA, it is cross-referenced with IDRS.

C. PRIVACY ACT AND SYSTEM OF RECORDS

9. Are 10 or more records containing SBU/PII maintained, stored, and/or transmitted by or through this system? Yes

9a. If **yes**, are records in the system retrieved by any personal identifier (e.g., name, SSN, Photograph, IP Address) for an individual? Yes

If **yes**, is there a System of Records Notice(s) or SORNs that addresses the PII records in this system? Yes

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

<u>SORNS Number</u>	<u>SORNS Name</u>
IRS 60.000	Employee Protection System
IRS 34.037	Audit Trail and Security Records System

If **yes**, does the System of Records Notice(s) (SORN) published in the Federal Register adequately describe the records as required by the Privacy Act? Yes

D. RESPONSIBLE PARTIES

N/A

E. INCOMING PII INTERFACES

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

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

No System Records found.

11b. 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).

<u>Organization Name</u>	<u>Transmission method</u>	<u>ISA/MOU</u>
TIGTA	EFTU	No

11c. Does the system receive SBU/PII from State or local agency (-ies)? No

No Organization Records found.

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

No Organization Records found.

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

No Tax Form Records found.

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

No Employee Form Records found.

F. PII SENT TO EXTERNAL ORGANIZATIONS

12. Does this system disseminate SBU/PII? Yes

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

No System Records found.

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

No Organization Records found.

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

<u>Organization Name</u>	<u>Transmission method</u>	<u>ISA/MOU</u>
--------------------------	----------------------------	----------------

various State and local	Secure email	No
-------------------------	--------------	----

Identify the authority and for what purpose? Inter-agency agreement (ISA) or Memorandum of Understanding (MOU)

G. PRIVACY SENSITIVE TECHNOLOGY

13. Does this system use social media channels? No

14. Does this system use privacy-sensitive technologies such as mobile, cloud, global position system (GPS), biometrics, 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/is notice provided to the individual prior to collection of information? No

17a. If **yes**, how is notice provided? Was the individual notified about the authority to collect the information, whether such is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects, if any, if they decide not to provide any of the requested information?

17b. 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

18b. If no, why not? The EPS database receives information daily from the Treasury Inspector General for Tax Administration (TIGTA). The Performance and Results Information System (PARIS) application sends data via SFTP to the GSS-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.

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

<u>IRS Employees?</u>	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

21a. 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

21b. If computer matching occurs, can the business owner certify that it meets requirements of IRM 11.3.39 Disclosure of Official Information, Computer Matching & Privacy Protection Act?

Yes

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

22a. 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 ECM-R

23. Has the system been through SA&A (Security Assessment and Authorization) or ECM-R (Enterprise Continuous Monitoring Reauthorization)? Yes

23a. If **yes**, what date was it completed? 6/13/2014 12:00:00 AM

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.

I.2 SA&A OR ECM-R

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

24b. If **yes**, is the test plan in process or completed: Completed

24.3 If **completed/ or in process**, 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?

Annual Continuous Monitoring TableTop Exercise FISMA 2015

24b.1. If **completed**, where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)? Yes, in FTIMS system

24b.2. If **completed**, were all the Privacy Requirements successfully tested? Yes

24.2 If **completed**, are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved? No

K. LIVE DATA TESTING

25. Does this system use, or plan to use Live Data in Testing? No

L. NUMBER AND CATEGORY OF PII RECORDS

26. Identify the number of individual records in the system for each category:

26a. IRS Employees:	<u>Not Applicable</u>
26b. Contractors:	<u>Not Applicable</u>
26c. Members of the Public:	<u>Under 100,000</u>
26d. Other:	<u>No</u>

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 9/11 Commission Recommendations 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

N. ACCOUNTING OF DISCLOSURES

30. Does the system include or require disclosure of tax or employee information to anyone other than IRS employees or IRS contractors 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

End of Report
