

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: 08/21/2014 PIA ID Number: 1030

1. What type of system is this? Legacy

1a. Is this a Federal Information Security Management Act (FISMA) reportable system? Yes

2. Full System Name, Acronym, and Release/Milestone (if appropriate):

Third Party Contact , TPC

2a. Has the name of the system changed? No

If yes, please state the previous system name, acronym, and release/milestone (if appropriate):

3. Identify how many individuals the system contains information on

Number of Employees: Not Applicable

Number of Contractors: Not Applicable

Members of the Public: Over 1,000,000

4. Responsible Parties:

NA

5. General Business Purpose of System

Third Party Contact (TPC) is designed to maintain a database of all third party contacts that were made regarding a taxpayer during the determination or collection of a tax liability. Each record on the database contains the contact name or general description of the third party contacted (ex. neighbour, bank name, business associate) along with the date of contact for all contacts made relating to a specific Taxpayer Identification Number (TIN). A third-party contact is made when an IRS employee initiates contact with a person other than the taxpayer. A third party may be contacted to obtain information about a specific taxpayer with respect to that taxpayer's Federal tax liability, including the issuance of a levy or summons to someone other than the taxpayer. TPC shares data with four (4) IRS applications but does not connect directly to each. Data from the Automated Collection System (ACS), Automated Under Reporter (AUR), Electronic Fraud Detection System (EFDS) and the Integration Collection System (ICS), are transferred to the GSS-21 IBM Mainframe on which TPC resides using the Electronic File Transfer Utility (EFTU). Once the IBM Mainframe receives data from the ACS, AUR, EFDS, and ICS applications, a batch job is executed which "pulls" the data that each application stored into the TPC database. TPC also receives data from various 12175 forms from which data is manually entered into the TPC database by TPC Coordinators. TPC receives weekly batch files of third party contacts from the ICS, ACS, AUR, and EFDS applications.

6. Has a PIA for this system, application, or database been submitted previously to the Office of Privacy Compliance? (If you do not know, please contact *Privacy and request a search) Yes

6a. If Yes, please indicate the date the latest PIA was approved: 08/10/2011

6b. If Yes, please indicate which of the following changes occurred to require this update.

- System Change (1 or more of the 9 examples listed in OMB 03-22 applies) (refer to PIA Training Reference Guide for the list of system changes) No
 - System is undergoing Security Assessment and Authorization Yes
-

6c. State any changes that have occurred to the system since the last PIA

There have been no changes to the Third Party Contact (TPC) system since the last SA&A.

7. If this system has an Exhibit 53 or Exhibit 300 please provide the Unique Project Identifier (UPI) number (XXX-XX-XX-XX-XX-XXXX-XX). Otherwise, enter the word 'none' or 'NA'. none

B. DATA CATEGORIZATION

Authority: OMB M 03-22 & PVR #23- PII Management

8. Does this system collect, display, store, maintain or disseminate Personally Identifiable Information (PII)? Yes

8a. If No, what types of information does the system collect, display, store, maintain or disseminate?

9. Indicate the category that best describes the source that provides or originates the PII collected, displayed, stored, maintained or disseminated by this system. Most common categories follow:

Taxpayers/Public/Tax Systems Yes

Employees/Personnel/HR Systems No

Other No

Other Source: _____

10. Indicate all of the types of PII collected, displayed, stored, maintained or disseminated by this system. Then state if the PII collected is on the Public and/or Employees. Most common fields follow:

TYPE OF PII	Collected?	On Public?	On IRS Employees or Contractors?
Name	Yes	Yes	No
Social Security Number (SSN)	Yes	Yes	No
Tax Payer ID Number (TIN)	No	Yes	No
Address	Yes	Yes	No
Date of Birth	No	No	No

Additional Types of PII: No

No Other PII Records found.

10a. Briefly describe the PII available in the system referred to in question 10 above.

Name and Address are part of the batch layout and as such are displayed.

If you answered Yes to Social Security Number (SSN) in question 10, answer 10b, 10c, and 10d.

10b. Cite the authority that allows this system to contain SSN's? (e.g. specific regulations, statutes, etc.)

IRC Section 7602(c)(2) and (3)

10c. What alternative solution to the use of the SSN has/or will be applied to this system? (e.g. masking, truncation, alternative identifier)

None

10d. Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of Social Security Numbers on this system?

Not applicable

11. Describe in detail the system's Audit Trail. State what data elements and fields are collected. Include employee log-in information. If the system does not have audit capabilities, explain why an Audit Trail is not needed.

Taxpayer: Taxpayer Identification Number (TIN) Secondary TIN Name Control Employee: ID Number, Telephone Number, Mail Stop Number Audit Trail Information: Date of Contact. Class 1 – Access attempts denied due to inadequate authorization (IFCID 140) Class 2 – Explicit GRANT and REVOKE (IFCID 141) Class 3 – CREATE, ALTER, and DROP operations against audited tables (IFCID 142) Class 4 – First change of audited object (IFCID 143) Class 5 – First read of audited object (IFCID 144) Class 6 – Bind time information about SQL statements involving audited objects (IFCID 145) Class 7 – Assignment or change of authorization IDs (IFCIDs 55, 83, 87, 169, and 319) Class 8 – Utilities (IFCIDs 23, 24, 25, 219, and 220) Other: Name of Third Party Reprisal Determination Category of Third Party Employee Plans (EP) Plan Number (Tax Exempt/Government Entities (TEGE) only) Master File Table (MFT)/Tax Year

11a. Does the Audit Trail contain the Audit Trail elements as required in current IRM 10.8.3 Audit Logging Security Standards? Yes

12. What are the sources of the PII in the system? Please indicate specific sources:

a. IRS files and databases: Yes

If Yes, the system(s) are listed below:

<u>System Name</u>	<u>Current PIA?</u>	<u>PIA Approval Date</u>	<u>SA & A?</u>	<u>Authorization Date</u>
Employee Plans Master File (EPMF))	Yes	05/02/2014	No	
Individual Master File (IMF)	Yes	05/02/2014	Yes	05/18/2011
Business Master File (BMF)	Yes	06/02/2014	Yes	03/12/2012

b. Other federal agency or agencies: No

If Yes, please list the agency (or agencies) below:

c. State and local agency or agencies: No

If Yes, please list the agency (or agencies) below:

d. Third party sources: Yes

If yes, the third party sources that were used are:

All information comes from IRS compliance officers.

e. Taxpayers (such as the 1040): No

f. Employees (such as the I-9): No

g. Other: No If Yes, specify:

C. PURPOSE OF COLLECTION

Authorities: OMB M 03-22 & Internal Revenue Manual (IRM) 10.8.8, IT Security, Live Data Protection Policy & PVR #16, Acceptable Use

13. What is the business need for the collection of PII in this system? Be specific.

The TPC application supports approximately 10,000 Small Business/Self-Employed, Wage & Investment, Appeals, and the Taxpayer Advocate Service end users. TPC provides an automated system for ROs, RAs, Group Managers, and support staff to collect and report pertinent information received from third party sources.

D. PII USAGE

Authority: OMB M 03-22 & PVR #16, Acceptable Use

14. What is the specific use(s) of the PII?

To conduct Tax Administration Yes

To provide Taxpayer Services No

To collect Demographic Data No

For employee purposes No

Other: No

If other, what is the use?

E. INFORMATION DISSEMINATION

Authority: OMB M 03-22 & PVR #14- Privacy Notice and #19- Authorizations

15. Will the information be shared outside the IRS? (for purposes such as computer matching, statistical purposes, etc.) No

15a. If yes, with whom will the information be shared? The specific parties are listed below:

	Yes/No	Who?	ISA OR MOU**?
Other federal agency (-ies)			
State and local agency (-ies)			
Third party sources			
Other:			

** Inter-agency agreement (ISA) or Memorandum of Understanding (MOU)

16. Does this system host a website for purposes of interacting with the public? No

17. Does the website use any means to track visitors' activity on the Internet?

If yes, please indicate means:

	YES/NO	AUTHORITY
Persistent Cookies	_____	_____
Web Beacons	_____	_____
Session Cookies	_____	_____
Other:	_____	_____

If other, specify:

F. INDIVIDUAL CONSENT

Authority: OMB M 03-22 & PVR #15- Consent and #18- Individual Rights

18. Do individuals have the opportunity to decline to provide information or to consent to particular uses of the information? Yes

18a. If Yes, how is their permission granted?

As the contact information is not being asked of the taxpayer the person being asked can decline to provide the requested information.

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

19a. If Yes, how does the system ensure "due process"?

The system will allow affective parties the opportunity to clarify or dispute negative information that could be used against them. Due process is provided pursuant to 5 USC.

20. Did any of the PII provided to this system originate from any IRS issued forms? Yes

20a. If Yes, please provide the corresponding form(s) number and name of the form.

No forms found.

20b. If No, how was consent granted?

Written consent	_____
Website Opt In or Out option	_____
Published System of Records Notice in the Federal Register	_____
Other:	_____

G. INFORMATION PROTECTIONS

Authority: OMB M 03-22 & PVR #9- Privacy as Part of the Development Life Cycle, #11- Privacy Assurance, #12- Privacy Education and Training, #17- PII Data Quality, #20- Safeguards and #22- Security Measures

21. Identify the owner and operator of the system: IRS Owned and Operated

21a. If Contractor operated, has the business unit provided appropriate notification to execute the annual security review of the contractors, when required?

22. The following people have use of the system with the level of access specified:

	Yes/No	Access Level
IRS Employees:	<u>Yes</u>	
Users		<u>Read Write</u>
Managers		<u>Read Only</u>
System Administrators		<u>Read Only</u>
Developers		<u>Read Only</u>
Contractors:	<u>No</u>	
Contractor Users		<u></u>
Contractor System Administrators		<u></u>
Contractor Developers		<u></u>
Other:	<u>No</u>	<u></u>

If you answered yes to contractors, please answer 22a. (All contractor/contractor employees must hold at minimum, a "Moderate Risk" Background Investigation if they have access to IRS owned SBU/PII data.)

22a. If the contractors or contractor employees act as System Administrators or have "Root Access", does that person hold a properly adjudicated "High Level" background investigation?

23. How is access to the PII determined and by whom?

Access to the TPC data is determined by a user's manager. Access is granted to individual employees on a "need to know" basis, and upon the successful completion of the On-Line 5081 (OL5081) process.

24. How will each data element of SBU/PII be verified for accuracy, timeliness, and completeness?

Data is visually inspected and corrected manually when errors are encountered.

25. 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

25a. 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.

TPC master data files are approved for deletion/destruction when 30 years old under National Archives Job No. N1-58-09-29. Data is archived to tape when 5 years old, the archived tape is destroyed when 25 years old. Disposition instructions are published in Records Control Schedule (RCS) Document 12990 under RCS 19 for Enterprise Computing Center –Martinsburg, item 53.

If No, how long are you proposing to retain the records? Please note, if you answered no, you must contact the IRS Records and Information Management Program to initiate records retention scheduling before you dispose of any records in this system.

26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.

TPC follows the concept of least privilege, and access controls are implemented according to IRM 10.8.1 to protect the confidentiality and integrity of information at rest; application administrator can only access information necessary to perform their job function. The application adheres to the SA&A and physical security requirements set forth in IRM 10.4.1- Physical Security Program- Managers Security Handbook

26a. Next, explain how the data is protected in the system at rest, in flight, or in transition.

All internal to IRS

27. Has a risk assessment (e.g., SA&A) been conducted on the system to ensure that appropriate security controls have been identified and implemented to protect against known risks to the confidentiality, integrity and availability of the PII? Yes

28. Describe the monitoring/evaluating activities undertaken on a regular basis to ensure that controls continue to work properly in safeguarding the PII.

TPC stakeholders meet prior to any major change being made to the TPC application or system environment. Before changes are made, they are evaluated against the business requirements, which are generated and approved by application stakeholders. Specific planning and coordination occurs before conducting security-related activities affecting the information system. Appropriate planning and coordination occurs between IT, Cybersecurity, and the TPC Stakeholders occur before conducting these activities to minimize the impact on TPC operations. On an annual basis, the business unit participates in the Enterprise Continuous Monitoring Exercises, including updates to the Information Security Contingency Plan (ISCP) and SSP. Every three years, TPC goes through the eCM-r process, which, in addition to the annual exercises, includes a comprehensive Security Control Assessment (SCA).

29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 - IT Security, Live Data Protection Policy? Yes

29a. Has approval been received from the Office of Privacy Compliance to use Live Data in testing (if appropriate)? No

29b. If you have received permission from the Office of Privacy Compliance to use Live Data, when was the approval granted? __/__/__

H. PRIVACY ACT & SYSTEM OF RECORDS

Under the statute, any employee who knowingly and willfully maintains a system of records without meeting the Privacy Act notice requirements is guilty of a misdemeanor and may be fined up to \$5000.

Authority: OMB M 03-22 & Privacy Act, 5 U.S.C. 552a (e) (4) & PVR #13-Transparency

30. Are 10 or more records containing PII maintained/stored/transmitted through this system? Yes

31. Are records on the system retrieved by any identifier for an individual? (Examples of identifiers include but are not limited to Name, SSN, Photograph, IP Address) Yes

31a. If YES, the System of Records Notice(s) (SORN) published in the Federal Register adequately describes the records as required by the Privacy Act? Enter the SORN number and the complete name of the SORN.

SORNS Number

SORNS Name

Treasury/IRS 00.333 Third Party Contacts

Treasury/IRS 00.334 Third Party Contact Reprisal Records

Treasury/ IRS 24.047 Audit Underreporter Case File

Treasury/IRS 34.037 IRS Audit Trail and Security Records Systems

I. ANALYSIS

Authority: OMB M 03-22 & PVR #21- Privacy Risk Management

32. What choices were made or actions taken regarding this IT system or collection of information as a result of preparing the PIA?

- Resulted in the removal of PII from the system (e.g., SSN use reduced/eliminated) No
- Provided viable alternatives to the use of PII within the system No
- New privacy measures have been considered/implemented Yes
- Other: No

32a. If Yes to any of the above, please describe:

New or improved privacy measures were discussed as part of the annual System Security Plan review. However given the current state of TPC none were deemed feasible at this time.

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