Third Party Contact (TPC) – Privacy Impact Assessment

PIA Approval Date – August 15, 2011

System Overview

The Third Party Contact (TPC) application 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. 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 Modernization & Information Technology Services (MITS)–21 General Support System (GSS) 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.

Systems of Records Notice (SORN):

- IRS 00.333--Third Party Contacts
- IRS 00.334--Third Party Contact Reprisal Records
- IRS 24.047--Audit Underreporter Case File
- IRS 34.037--IRS Audit Trail and Security Records Systems

Data in the System

1. Describe the information (data elements and fields) available in the system in the following categories:

A. Taxpayer:
- Taxpayer Identification Number (TIN)
- Secondary TIN
- Name Control

B. Employee:
- ID Number
- Telephone Number
- Mail Stop Number

C. 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 Structured Query Language (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)

D. 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

2. Describe/identify which data elements are obtained from files, databases, individuals, or any other sources.

A. IRS: Data elements include:
- TIN
- Social Security Number (SSN)
- Name Control

All data elements are obtained from:
- ACS
- AUR
- EFDS
- ICS

Data in ACS, AUR, EFDS, and ICS, are obtained two ways:
- Third Party Contact Form 12175 are completed by IRS employees and entered by TPC coordinators using Integrated Data Retrieval System (IDRS) command codes
- Other IRS files

Taxpayer data elements (TIN, SSN, and Name Control) may also come from IRS compliance officers who work TPC cases, and provide the information to IRS revenue agents.

B. Taxpayer: TPC Coordinators do not receive any information directly from taxpayers. All information comes from IRS compliance officers.

C. Employee: Data elements are provided by IRS compliance employees to designated TPC Coordinators for use in entering into the TPC database. Certain IRS compliance employees are responsible for the automated process of entering data into the database, while TPC Coordinators are responsible for the manual process using Form 12175.

3. Is each data item required for the business purpose of the system? Explain.
Yes, each data item is required for the business purpose of the system. Section 3417 of the Internal Revenue Service Restructuring and Reform Act of 1998 amended Internal Revenue Code (IRC) Section 7602(c)(2) and (3) states that the Service is to provide the taxpayer a record of persons contacted with respect to the determination or collection of the tax liability. It also identifies exceptions to providing a record of persons contacted because of reprisal against any person, pending criminal investigation, authorization by taxpayer, or jeopardizing tax collection. The data items provide the Service with the ability to identify the taxpayer who is requesting a record of person(s) contacted, the person(s) contacted as well as person(s) exempt per IRC 7602(c)(3).

4. How will each data item be verified for accuracy, timeliness, and completeness?
TPC only accepts valid values. TPC utilizes the NAP application to perform a validity check on the Name Control and the TIN for all data coming into TPC from ICS, ACS, EFDS, and AUR. If there is a match, the contact can be processed. If the Name Control and TIN do not match, then the contact is

added to a "reject" to be re–worked. In addition, Third Party Contact coordinators review information for accuracy and completeness before input.

5. Is there another source for the data? Explain how that source is or is not used.
No, TPC has no other sources for the data.

6. Generally, how will data be retrieved by the user?
The user will use the IDRS and Command Code TPCOL to retrieve data in the system.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?
Yes, data is retrievable by using the TIN that was initially entered in the system.

Access to the Data

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?
TPC users are assigned to one of two (2) end user groups: (i) Coordinators and (ii) Supervisors. Only TPC Coordinators and Supervisors have access to the TPC application and data. The Modernization & Information Technology Services (MITS) Information Technology (IT) Support team provides infrastructure (system and database administration) and programming support to the TPC application. Currently, no contractors have access to TPC data.

> **Roles:** Coordinators
> **Permissions:** Coordinators maintain the originator's Form 12175 (the form from which data is entered into the TPC database), verify its completeness, enter its data into the TPC database, and respond to requests from taxpayers for a list of third–party contacts. They access TPC after entering IDRS command codes and are authenticated by the Security and Communication System (SACS).

> **Roles:** Supervisors
> **Permissions:** Supervisors have similar privileges as coordinators, and in addition, oversee multiple coordinators. Their access to the TPC application is similar to Coordinators.

> **Roles:** Modernization & Information Technology Services (MITS) IT Support
> **Permissions:** MITS Information Technology (IT) Support consists of system/database administrators and developers. Users of this group maintain the system on which TPC resides (system administrators), the database (database administrators), and make necessary updates/modifications to the application when required (developers).

9. How is access to the data by a user 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.

10. Do other IRS systems provide, receive, or share data in the system? If YES, list the system(s) and describe which data is shared.
Yes. Information is obtained from the following:
- Automated Collection System (ACS)
- Automated Under Reporter (AUR)
- Electronic Fraud Detection System (EFDS)

- Integration Collection System (ICS)

11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?
Yes.
Automated Collection System (ACS)
- Certification & Accreditation (C&A) – May 25, 2010
- Privacy Impact Assessment (PIA) – December 28, 2009

Automated Underreporter (AUR)
- Certification & Accreditation (C&A) – May 6, 2009
- Privacy Impact Assessment (PIA) – February 27, 2009

Electronic Fraud Detection System (EFDS)
- Certification & Accreditation (C&A) – June 14, 2011
- Privacy Impact Assessment (PIA) – December 17, 2010

Integrated Collection System (ICS)
- Certification & Accreditation (C&A) – May 19, 2011
- Privacy Impact Assessment (PIA) – December 15, 2010

12. Will other agencies provide, receive, or share data in any form with this system?
No, other agencies will not provide, receive, or share data in any form with this system.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?
TPC master data files are approved for deletion/destruction when 30 years old. Data is archived to tape when 5 years old, the archived tape is destroyed when 25 years old. The National Archives and Records Administration (NARA) approved these disposition instructions under Job No. N1–58–09–29 (approved 8/25/09). These instructions are published under IRM 1.15.19 Records Control Schedule for Enterprise Computing Center–Martinsburg (ECC–MTB), Item 53.

14. Will this system use technology in a new way?
No, the TPC application will not use technology in a new way.

15. Will this system be used to identify or locate individuals or groups? If so, describe the business purpose for this capability.
Yes, TPC can be used to identify the third party contacts. Since January 18, 1999, the IRS has been required to inform the taxpayer of the possibility that third–parties may be contacted in connection with the determination or collection of a tax. All IRS employees who contact third–parties in connection with the determination or collection of a tax must keep a complete and accurate record of the third–party contact. Upon request, the Service will provide the taxpayer with a record of the persons contacted and will also provide this information whenever the taxpayer requests it. See Internal Revenue Code 7602(c). Section 7602(c) does not apply if the contacts are made pursuant to a criminal investigation or if the Service determines that releasing the information would either jeopardize tax collection or subject the third–party to reprisals. In addition, this section does not apply to any contact authorized by the taxpayer.

16. Will this system provide the capability to monitor individuals or groups? If yes, describe the business purpose for this capability and the controls established to prevent unauthorized monitoring.

No, TPC does not provide the capability to monitor individuals or groups.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?

No, the system does not allow IRS to treat taxpayers, employees, or others, differently. The purpose of the TPC application is to store and retrieve data on third party contacts made by IRS employees who are in the process of examining or collecting tax liabilities from an individual or business entity.

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

Not applicable, the purpose of the TPC application is to store and retrieve data on third party contacts made by IRS employees who are in the process of examining or collecting tax liabilities from an individual or business entity.

19. If the system is web–based, does it use persistent cookies or other tracking devices to identify web visitors?

Not applicable, TPC is not a web–based application.

View other PIAs on IRS.gov