Date of Approval: June 05, 2017 PIA ID Number: **2560**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Third Party Contact, TPC

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, PIA ID Number and milestone of the most recent PIA.

Third Party Contact, PIAMS # 935

Next, enter the **date** of the most recent PIA. 08/22/2014

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
No	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? Yes

If yes, explain what changes were made. Current PIA is expiring in August 2017.

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? No

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.

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. neighbor, 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

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

6a. 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 who the SSN (or tax identification number) is collected on.

Yes	On Primary	No	On Spouse	No	On Dependent

If **yes**, check all types SSN s (or tax identification numbers) that apply to this system:

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

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 memorandum M-07-12 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. The TPC system requires the use of SSN’s because no other identifier can be used to uniquely identify a taxpayer at this time. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns.

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

If **yes**, specify the information.

On Primary	On Spouse	On Dependent	Selected	PII Element
Yes	Name	Yes	No	No
Yes	Mailing address	No	No	No
No	Phone Numbers	No	No	No
No	E-mail Address	No	No	No
No	Date of Birth	No	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
No	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

6c. 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.
No	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
No	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
No	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)

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

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 tax identification numbers) are used, explicitly explain why use of SSNs meets this criteria. Be specific.

The Third-Party Contact System 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. neighbor, bank name, business associate) along with the date of contact for all contacts made relating to a specific TIN. (1) Taxpayer TIN is used to uniquely identify the taxpayer, and is required as the only identifier that is possible in order to verify a match against the National Account Profile (NAP), where the record key is TIN. (2) Likewise, the taxpayer name control is used on the site. The name control generally consists of the first four characters of a taxpayer's last name. The National Account Profile maintains current and prior name controls, and uses name controls as further authentication and matching of the taxpayer. The name control must be provided in order to authenticate the taxpayer in question with the associated TIN.

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

Data is visually inspected and corrected manually when errors are encountered There are internal programming consistency checks and record counts to validate the data that is loaded into the TPC system is accurate. The data that TPC receives is from internal IRS systems which are deemed reliable and the data is validated for accuracy by the system sending the data as described in that system's PCLIA. Following NAP validation in the TPC system, further determinations may be made by Collection and Compliance Processing, but no determinations are made by the Third-Party Contact NAP program. The taxpayer has subsequent appeal rights for any return selected for Collection or Examination

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.

SORNS Number	SORNS Name
IRS 00.333	Third Party Contact Records
IRS 00.334	Third Party Contact Reprisal Records
IRS 24.047	Audit Underreporter Case Files
IRS 34.037	Audit Trail and Security Records Systems

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

10. Identify the individuals for the following system roles.

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? Yes

If **yes**, enter the files and databases.

System Name	Current PCLIA	Approval Date	SA&A?	Authorization Date
Automated Underreporter	Yes	06/06/2016	Yes	09/21/2016
Integrated Collection System	Yes	05/05/2016	Yes	09/25/2016
Electronic Fraud Detection System	Yes	12/01/2013	Yes	11/29/2016
Automated Collection System	Yes	12/18/2015	Yes	12/14/2016

11b. Does the system receive SBU/PII from other federal agency or agencies? No

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

11d. Does the system receive SBU/PII from other sources? Yes

If **yes**, identify the source 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
Tax Compliance officers	systematically	No

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

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

F. PII SENT TO EXTERNAL ORGANIZATIONS

12. Does this system disseminate SBU/PII? 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, 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? Yes

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?
The IRS notifies all individuals who file tax returns of such collection via the Privacy Act Notice in tax return instructions. When a return is selected for Examination, Collection etc., the taxpayer is sent the Privacy Act Notice, Your Appeals Rights and How to Prepare a Protest and Overview of the Appeals Process. Per OMB Privacy Act Guidelines at 28961, it is understood that to the greatest extent practicable, Federal program decisions be made based on information supplied by the individual about whom the decision is made. However, the rule also recognizes that it may not always be practical to consult the individual before making a determination that may affect them. This is also noted on page 9 of the Treasury Privacy Act Handbook: Since information collected from a third-party source could be erroneous, irrelevant, or biased, subsection (e)(2) of the Act provides that determinations which may adversely affect an individual's rights, benefits and/or privileges under a Federal program be made on the basis of information supplied by the record subject when practicable. One of the factors considered when using a third-party source is that the nature of the program (e.g., criminal or terrorism investigations) makes it impossible to get the information from the individual, such as in the case of a tax investigation for purposes of collection or a compliance investigation. The taxpayer is not asked to provide contact information, and the third party being asked can decline to provide the requested information.

18. Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information? Yes

18a. If **yes**, describe the mechanism by which individuals indicate their consent choice(s):
All individuals have the right to decline to provide information. However, they may be subject to Examination or Deficiency procedures, at which time they are provided applicable notices, such as Your Appeals Rights and How to Prepare a Protest.

19. How does the system or business process ensure due process regarding information access, correction and redress?
The Third-Party Contact process and procedures are dictated by the Internal Revenue Manual guidelines. IRS policy allows individuals whose data is in the system the opportunity to clarify or dispute negative determinations through the appeals process.

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 and Write
Sys. Administrators	Yes	Read-Only
Developers	Yes	Read-Only

Contractor Employees? No

21a. How is access to SBU/PII determined and by whom? The TPC system utilizes the IRS OL-5081 application to document approvals for access. Data access is granted on a need-to-know basis. A potential user must submit a request for access via IRS On–Line application 5081 (OL5081) to their local management for approval consideration. Users are not permitted access without a signed 5081 form from an authorized management official. Specific permissions (Read, Write, Modify, Delete, and/or Print) are defined on the OL5081 form and set (activated) by the System Administrator prior to the user being allowed access. User privileges and user roles determine the types of data that each user has access to. Management monitors system access and removes permissions when individuals no longer require access.

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?

Not Applicable

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.

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.

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? 11/04/2015

23.1 Describe in detail the system s audit trail. The audit trail contains the audit trail elements as required in current IRM 10.8.3, Audit Logging Security Standards, The data elements contain the Taxpayer Identification Number (TIN) Secondary TIN Name Control, the Employee ID Number, Telephone Number, and Mail Stop Number. The Audit Trail Information is the 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.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? No

24c. If **no**, please explain why. Non FISMA Reportable for FY17 due to reclassification to Tier 4.

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:

26a. IRS Employees: Not Applicable
26b. Contractors: Not Applicable
26c. Members of the Public: More than 1,000,000
26d. 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 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? Yes

If **yes**, describe the type of information derived from these efforts and the technical (e.g., audit trails) or other processes used to limit unauthorized monitoring. 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

N. ACCOUNTING OF DISCLOSURES

30. 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? No

End of Report