Date of Approval: **March 29, 2020**

PIA ID Number: **4892**

SYSTEM DESCRIPTION

Enter the full name and acronym for the system, project, application and/or database.

Third Party Contact, TPC

Is this a new system?

No

Is there a PCLIA for this system?

Yes

What is the full name, acronym and milestone of the most recent PCLIA?

Third Party Contact, TPC, PIA ID Number 2560

What is the approval date of the most recent PCLIA?

6/5/2017

Changes that occurred to require this update:

Expiring PCLIA

Were there other system changes not listed above?

Yes

What were those changes?

Current PCLIA expiring May 2020.

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

SBSE Risk Committee

Current ELC (Enterprise Life Cycle) Milestones:

Operations & Maintenance (i.e. system is currently operational)

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

No

GENERAL BUSINESS PURPOSE

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 Forms 12175 (Third Party Contact Report 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.

PII DETAILS

Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any other type of Sensitive but Unclassified (SBU) information or PII such as information about IRS employees or outside stakeholders?

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

What types of tax identification numbers (TIN) apply to this system?

Social Security Number (SSN)

List the approved Treasury uses of the SSN:

Legal/statutory basis (e.g. where collection is expressly required by statute)

Law enforcement and intelligence purposes

Explain why the authorized use(s) above support the new or continued use of SSNs (or tax identification numbers)

A legal basis exists to collect the information, as 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. The IRS is required to make record of those contacted during the investigation or collection of tax liability, and the SSN is uniquely needed to identify a user's record.

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 Circular A-130 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.

Employer Identification Number

Other Taxpayer Identification Number

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

Yes

Specify the PII Elements:

Name

Mailing address

Phone Numbers

Tax Account Information

Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?

Yes

Specify the types of SBU from the SBU Types List

Agency Sensitive Information Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission

Are there other types of SBU/PII used in the system?

No

Cite the authority for collecting SBU/PII (including SSN if relevant

PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, & 6012e(a)

SSN for tax returns and return information is Internal Revenue Code Section 6109

Has the authority been verified with the system owner?

Yes

BUSINESS NEEDS AND ACCURACY

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 (Taxpayer Identification Number). (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.

How is the SBU/PII verified for accuracy, timeliness and completion?

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.

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.

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

Identify the Privacy Act SORN(s) that cover these records.

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

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

Official Use Only

INCOMING PII INTERFACES

Does the system receive SBU/PII from other systems or agencies?

Yes

Does the system receive SBU/PII from IRS files and databases?

Yes

Enter the files and databases:

System Name: National Account Profile
Current PCLIA: Yes
Approval Date: 2/27/2020
SA&A: No

System Name: Automated Underreporter
Current PCLIA: Yes
Approval Date: 6/12/2019
SA&A: Yes
ATO/IATO Date: 11/1/2019

System Name: Integrated Collection System
Current PCLIA: Yes
Approval Date: 5/14/2019
SA&A: Yes
ATO/IATO Date: 4/4/2019

System Name: Electronic Fraud Detection System
Current PCLIA: Yes
Approval Date: 1/10/2018
SA&A: Yes
ATO/IATO Date: 3/27/2020

System Name: Automated Collection System
Current PCLIA: Yes
Approval Date: 10/12/2018
SA&A: Yes
ATO/IATO Date: 11/6/2018

Does the system receive SBU/PII from other federal agency or agencies?

No

Does the system receive SBU/PII from State or local agency (-ies)?

No

Does the system receive SBU/PII from other sources?

No

Does the system receive SBU/PII from Taxpayer forms?

No

Does the system receive SBU/PII from Employee forms (e.g. the I-9)?

Yes

Please identify the form number and name:

Form Number: Form 12175 Form Name: Third Party Contact

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

No

PRIVACY SENSITIVE TECHNOLOGY

Does this system use social media channels?

No

Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.?

No

Does the system use cloud computing?

No

Does this system/application interact with the public?

No

INDIVIDUAL NOTICE AND CONSENT

Was/is notice provided to the individual prior to collection of information?

Yes

How is notice provided? Was the individual notified about the authority to collect the information, whether disclosure is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects on the individual, if any, if they decide not to provide all or 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.

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

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.

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.

INFORMATION PROTECTION

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

The following people have access to the system with the specified rights:

IRS Employees

Users: Read Write

Managers: Read Write

System Administrators: Read Only

Developers: Read Only

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.

RECORDS RETENTION SCHEDULE

Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) approved a Records Control Schedule (RCS, IRS Document 12990) for the retention and destruction of official agency records stored in this system?

Yes

How long are the records required to be held under the corresponding GRS or RCS, and how are they disposed of? In your response, please provide the GRS or RCS chapter number, the specific item number, and records series 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.

SA&A OR ASCA

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

Yes

What date was it completed?

11/4/2015

Describe the system's audit trail.

Audit trail elements are referenced in 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, Employee Telephone Number, and Mail Stop Number. The Audit Trail Information is the Date of Contact.

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

Third Party Contact is a sub-program of the National Account Profile (NAP) Project. Testing is completed therefore as part of the NAP Test Plan, and Third Party does not have a separate Strategic Data Plan (SDP).

SBU DATA USE

Does this system use, or plan to use SBU Data in Testing?

No

NUMBER AND CATEGORY OF PII RECORDS

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

IRS Employees: Not Applicable

Contractors: Not Applicable

Members of the Public: More than 1,000,000

Other: No

CIVIL LIBERTIES

Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment?

No

Is the system information used to conduct 'data-mining' as defined in the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?

No

Will this system have the capability to identify, locate, and monitor individuals or groups of people?

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.

Does computer matching occur?

No

ACCOUNTING OF DISCLOSURES

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