Date of Approval: **June 08, 2022**

PIA ID Number: **6894**

SYSTEM DESCRIPTION

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

Third-Party Media Research Pilot, TPMR

Is this a new system?

Yes

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

The TPMR project reports to the Small Business Self Employed (SB/SE) Tech Governance Board, and the Digital Solutions Advisory Committee (DSAC)

Current ELC (Enterprise Life Cycle) Milestones:

Vision & Strategy/Milestone 0

Project Initiation/Milestone 1

System Deployment/Milestone 5

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 Media Research (TPMR) Solution is a project managed by SB/SE Technology Solutions and to obtain a Commercial Off-The Shelf (COTS) available third-party data tool that recognizes, collects, and ranks current and archived content from public facing media platforms to expedite IRS case resolution for existing tax compliance cases. TPMR Solution project consisted of a 90-day pilot that ended on January 29, 2022. The vendor is a license research tool that instantly builds comprehensive, court-ready, digital reports on businesses and people, collecting and analyzing publicly available information from data sources including social media, the dark web, associated vehicles, court records, and contact data. The tool would benefit the IRS in providing an efficient way of locating assets, and resources, assisting with the collection of known tax deficiencies, leading to increased

collection of revenue involving unpaid assessed liabilities, unfiled returns, closure of the tax gap and may assist to identify indicators of fraud. Adoption of research solution requires Directorate decision to either move forward with procuring a solution for SB/SE or advance a decision for the Deputy Commissioner for Services and Enforcement (DCSE) approval of an enterprise-wide solution. This process follows IRS policy on Use of Social Networking and Other Internet Sites by IRS Employees for Compliance Research or for Other Purposes found in IRM 11.3.21.8.1.

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)

When there is no reasonable alternative means for meeting business requirements

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

Use of the SSN on tax returns and tax return information is compliant with Internal Revenue Code IRC) Section 6109.

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

No planned mitigation strategy

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
E-mail Address
Date of Birth
Place of Birth
Criminal History
Medical Information
Certificate or License Numbers
Vehicle Identifiers
Photographic Identifiers
Biometric Identifiers
Employment Information

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

No

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 TPMR Project is based on the IRS need to build efficient agile compliance operations. To secure positive outcomes, we must search public facing data with the available SBU/PII data, such as name, address, phone numbers. A TPMR solution will expedite case resolution for existing tax compliance cases, providing more avenues to identify and locate taxpayers, business entities, assets and resources, and overall assistance with tax administration. In addition to the collection of known tax deficiencies, and returns, a solution can also assist to identify indicators of fraud, as well as be part of a comprehensive plan to close the tax gap. A vendor supplied solution gives authorized IRS personnel access to public facing, third-party data from any location. We are only gathering public information as it relates to assigned casework. Use of this research tool provides a fuller understanding of a taxpayer's public, self-identified, online presence while complying with IRS internet research policy guidelines.

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

Using SBU/PII we can check against results provided. New information is verified against existing known case data provided from internal sources or taxpayer provided data such as returns, W2s, paystubs etc.

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 00.002 Correspondence Files: Inquiries about Enforcement Activities

IRS 26.019 Taxpayer Delinquent Account Files

IRS 26.020 Taxpayer Delinquency Investigation Files

IRS 42.001 Examination Administrative Files

IRS 42.021 Compliance Programs and Projects Files

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?

No

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?

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: The Internet
Transmission Method: Data is aggregated into a report by an algorithm, which ranks data and pulls it into a report.
ISA/MOU: 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)?

No

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.?

Yes

Briefly explain how the system uses the referenced technology.

A search on publicly available third-party media sources, may bring back a wide range of public information put out on the internet voluntarily by an individual or business. The search results may return location, photo, video, or other types of third-party information that the individual or entity chose to make public.

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?

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.

Internet research does not require a third-party notification to the taxpayer. However, taxpayers are notified of their rights as a taxpayer and the compliance process via notices sent to them as their cases are created. In compliance situations, we must rely on third party sources to verify information provided by taxpayers and to find information taxpayers did not offer.

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

No

Why not?

The data collected is public information and does not require a need for consent.

How does the system or business process ensure 'due process' regarding information access, correction, and redress?

The compliance process allows for due process in the form of Collection Due Process (CDP) and 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).

Contractor Owned and Operated

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

IRS Employees

Users: Read Only

IRS Contractor Employees

Contractor Managers: Administrator

Contractor System Administrators: Administrator

Contractor Developers: Administrator

How is access to SBU/PII determined and by whom?

The vendor sees the activity of the logged in user, the reports, the number of reports, and the number of downloaded reports. The customer service representatives can see data to assist with inquiries and the administrative staff sees reports for audit trails. They do not see the details of the reports. Access to data is based on the approved security rules, determined by individual roles and responsibilities, and is restricted to "need to know." Users will follow established IRS procedures for access using Business Entitlement Access Request System (BEARS) and rules described in Unauthorized Access (UNAX). Information within the tool is protected from unauthorized access by a user login and strong password. Once the

information from the tool goes into a case file, authorized IRS personnel protect the information from unauthorized access and disclosure as required by the Internal Revenue Code. Though the data we are interested in securing, is public facing, and available, only because taxpayers and business entities have put the information into the public sphere themselves, the IRS acknowledges, once data is brought into a case, the data shall be treated as private to the taxpayer and any online research would be subject to UNAX guidelines.

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.

GRS 5.2 Item 020-Intermediary records. Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.

SA&A OR ASCA

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

No

Is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements?

Yes

Describe the system's audit trail.

Each user has a unique log in and strong password. All inquiries and work conducted while in the vendor supplied tool creates an audit trail that can be pulled on request.

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

This is a vendor supplied tool.

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: Under 50,000

Contractors: Under 5,000

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?

Yes

Explain the First Amendment information being collected and how it is used.

Public statements made by taxpayers may be returned via search inquiries of this publicly available information. These statements may qualify as protected First Amendment activities. This information may be used to identify individuals, businesses, and in the administration of current tax law, identifying assets, closure of the tax gap, collection of returns and identification of indicators of fraud. No adverse actions are ever taken against individuals based solely upon their exercise of First Amendment rights.

Please list all exceptions (any one of which allows the maintenance of such information) that apply:

The information maintained is pertinent to and within the scope of an authorized law enforcement activity (as noted in Q7).

There is a statute that expressly authorizes its collection (identified in Q6).

Will the First Amendment information be used as the basis to make any adverse determination about an individual's rights, benefits, and/or privileges under Federal programs?

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.

Publicly available information may be returned via search inquiries of public voluntary information posted by individuals or businesses. Information may be used in the compliance process to identify and locate - but not to monitor individuals, businesses, assets, and data in the administration of current tax law. Information may assist in identifying assets, closure of the tax gap, collection of returns and identification of badges of fraud. No additional monitoring of individuals takes place.

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