Tax Professional Preparer Tax Identification Number (PTIN) System (TPPS) – Privacy Impact Assessment

PIA Approval Date – Mar. 1, 2011

System Overview:
The Taxpayer Professional Preparer Tax Identification Number (PTIN) System (TPPS) application is a web–based application that will be used by approximately 900,000 to 1.2 million tax return preparers. The TPPS application's main business goals are to facilitate taxpayer compliance and ensure uniform and high ethical standards of conduct for tax preparers.

Systems of Records Notice (SORN):
- IRS 37.111--Preparer Tax Identification Number Records
  (The PTIN records will be covered by the Preparer Tax Identification Number System of Record (SOR) whose reports and notices have been drafted and will be published as soon as possible.)

Data in the System

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

A. Taxpayer – For TPPS, the "taxpayer" is the tax preparer and/or applicant. Online application data fields that the applicant/preparer will supply include:
- Social Security number (SSN)
- Name
- Date of Birth
- Tax Year of Previous Tax Return
- Address from Previous Tax Return
- Filing Status from Previous Tax Return

These data fields will be used for identification Proofing/Authentication purposes. If the Vendor receives a "pass" response from the IRS, the following data fields will be collected from the applicant/preparer:
- Other Addresses (Permanent Mailing/Business Location)
- Phone Numbers (Personal/Business)
- Doing Business As (DBA is the official acronym)
- Email Address
- Business Website Address
- Employer Identification Number (EIN)
- Centralized Authorization File (CAF) Number
- Electronic Filing Identification Number (eFIN)
- Whether a Responsible Official for an eFIN
- Professional Certification as an Attorney, Certified Public Accountant (CPA), Enrolled Agent, Enrolled Actuary and/or Enrolled Retirement Plan Agents (ERPA) that includes any associated licensing numbers and applicable states)
- Information on State Licensing for Preparation of returns that includes any associated licensing numbers – currently only applicable for four states)
- Felony Convictions (past 10 years)
- Federal Tax Compliance

B. Employee – Vendor Customer Service Reps (CSRs), and IRS authorized users (not yet identified) will have secure remote access with multiple tier accesses with associated permissions; data fields will consist of those used to set up their token accounts.

C. Audit Trail Information – The audit trail will capture the user ID of any individual that alters data per his/her permissions, the action taken, and a timestamp of when that action occurred.

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

A. IRS – personnel will have access to all data fields captured at time of application. All data is submitted by either the applicant/preparer/taxpayer; or the testing vendor (when one is secured).

B. Taxpayer (Preparer) – the preparer will be supplying the following information that populates the data fields within the database (those marked with an * are mandatory fields):
- First Name*
- Middle Name
- Last Name*
- SSN* (must be nine digits)
- Date of Birth* (must be entered in mm/dd/yyyy format)
- Address On US Individual Tax Return*
- Preferred e–mail Address*
- Permanent Mailing Address*
- Country (if they reside outside of the US)
- Telephone Number* (captured when we ask for permanent mailing address information – so, most likely home or cell)
- Telephone Number Extension (if applicable)
- Tax Year* (they have to identify which return they are pulling information from and must be entered in yyyy format)
- Filing Status*
- Felony Conviction in Past 10 Years* (must provide an explanation if they answer yes to a conviction)
- Tax Compliance* (must provide an explanation if they answer they are not in compliance)
- Professional Credentials (CPA, Attorney, Enrolled Agent, etc.)
- Identification of Self–Employed/Owner/Corporate Officer* (simple yes or no question)
- EFIN (if applicable and must be entered in proper EFIN format)
- Employer ID Number (if applicable and must be nine digits)
- CAF Number (if applicable and must be entered in proper CAF format)
- Doing Business As (if applicable)
- Business Address
- Country (if they do business outside of the US)
- Telephone Number (captured when we ask for business information)
- Telephone Number Extension (if applicable)

C. Employee – Vendor CSRs will have access to all data fields captured at time of application

3. Is each data item required for the business purpose of the system? Explain.
Every data item captured on the registration system is necessary for the business purpose of the system, whether for Authentication/ID Proofing, or for future compliance/enforcement use.

4. How will each data item be verified for accuracy, timeliness, and completeness?
Here are the data fields (same as above), those marked with an * are mandatory fields.
- First Name*
- Middle Name
- Last Name*
- SSN* (must be nine digits)
- Date of Birth* (must be entered in mm/dd/yyyy format)
- Address On US Individual Tax Return*
- Preferred e–mail Address*
- Permanent Mailing Address*
- Country (if they reside outside of the US)
- Telephone Number* (captured when we ask for permanent mailing address information – so, most likely home or cell)
- Telephone Number Extension (if applicable)
- Tax Year* (they have to identify which return they are pulling information from and must be entered in yyyy format)
- Filing Status*
- Felony Conviction in Past 10 Years* (must provide an explanation if they answer yes to a conviction)
- Tax Compliance* (must provide an explanation if they answer they are not in compliance)
- Professional Credentials (CPA, Attorney, Enrolled Agent, etc.)
- Identification of Self–Employed/Owner/Corporate Officer* (simple yes or no question)
- EFIN (if applicable and must be entered in proper EFIN format)
- Employer ID Number (if applicable and must be nine digits)
- CAF Number (if applicable and must be entered in proper CAF format)
- Doing Business As (if applicable)
- Business Address
- Country (if they do business outside of the US)
- Telephone Number (captured when we ask for business information)
- Telephone Number Extension (if applicable)
- Business Web Site

Data elements used for authentication are verified against internal IRS records through Return Preparer Registration–Identity Verification Service (RPR–IVS). Formatting around several data elements is defined by existing format rules found within IRS–issued numbers. For example: EIN, CAF, and EFIN are restricted to the number/character value currently associated with such identifying numbers. For those fields that have a format rule associated, the applicant can not move forward within the application and/or gain a PTIN without those fields being entered correctly. And, while formatting rules may apply to several fields, there is currently no "verification" associated with those fields. There is no timeliness associated with the data fields – although, if an application fails to authenticate prior year tax information 3–times within a 24–hour period then they cannot try again to obtain their PTIN until that 24–hour period has expired.

5. Is there another source for the data? Explain how that source is or is not used.

Yes, there is another source of data for the system. A data extract of information from the Legacy PTIN database will be shared one time with the vendor to allow an existing PTIN to be reassigned to an applicant after they have passed Authentication/ID Proofing.

Additionally, three other lists will be shared with the vendor that contain SSN information and which will lead to either a systemic revocation of an existing PTIN and/or the non–issuance of a PTIN when they apply. These lists are as follows:
- Injunctions (from Lead Development Center)
- Felony/Criminal Convictions (from Criminal Investigation)
- Suspensions/Disbarments from Office of Personnel Records (OPR), and not available until post January 2011)

6. Generally, how will data be retrieved by the user?
Data is accessible on the database itself by CSRs, and authorized IRS personnel. Additionally, reports will be available both in standard format and via ad hoc needs.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?
Yes. Data is retrievable by either an SSN or PTIN or any other data field where we have captured data from the applicant, and possibly in the future from the Testing Vendor.

Access to the Data

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?
TPPS is a Government–owned and a Contractor–operated application. Users, Managers, authorized IRS personnel, and Treasury Inspector General for Tax Administration (TIGTA) personnel have access to the system. In addition, system administrators and developers manage the application and are contractor personnel. See below for more information:

Role: Taxpayer/Applicant/Tax Preparer
Permission: Establishes a user account on the system, submits application for a PTIN, and has an ability to update the information they provide on either the application or updating supplemental information, such as Continuing Education credits earned.

Role: IRS End User
Permission: Specific IRS personnel will have access to the system with authority to do any or all of the following:
- work PTIN–related cases forwarded to the IRS for review, "revoke" or otherwise update the status of an assigned PTIN,
- Develop and pull standardized and adhoc reports, and
- query/review system data in a read only format.

Role: Treasury Inspector General for Tax Administration (TIGTA)
Permission: Will have access to all system information for auditing purposes in a query/read only format.

Role: Contractor Personnel

Permission: Customer Service Representatives (CSRs), team leads and managers will have access to the system in the same basic capacity as IRS users. System administrators and developers will have access to the system to update/maintain system processes.

9. How is access to the data by a user determined and by whom?
The TPPS Project Office will identify authorized IRS personnel, TIGTA will identify who in their organization will have access and share that with the Related Party Interest Project Office (RPI PO), and CSRs, their managers, etc., on the Vendor side will be determined by the Vendor. This is still being defined within the Project Office.

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, TPPS will share a copy of the following data fields with the Return Preparer Registration–Identity Verification Service (RPR–IVS) application to authenticate an individual:
- First Name
- Middle Name
- Last Name
- SSN (must be nine digits)
- Date of Birth
- Address On US Individual Tax Return*
- Tax Year from Previous Return
- Filing Status

11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?
Return Preparer Registration–Identity Verification Service (RPR–IVS) is currently running in the Integrated Customer Communications Environment (ICCE). ICCE is currently undergoing its own Security Assessment & Authorization (SA&A) and Privacy Impact Assessment (PIA) process.

12. Will other agencies provide, receive, or share data in any form with this system?
Yes, other state and local government agencies are provided a quarterly extract of the some basic PTIN information, i.e. PTIN and SSN. These agencies must request access through the Governmental Liaison Data Exchange Program. Those agencies are as follows:
- City Of Philadelphia – Department Of Revenue
- City Of Cincinnati
- Lexington–Fayette Urban County Government
- Central Collection Agency (CCA)
- Maine Revenue Services
- New Hampshire Dept Revenue
- Massachusetts Department Of Revenue
- Rhode Island Division Of Taxation
- New York State Department Of Taxation And Finance
- Division Of Taxation
- Pennsylvania Department Of Revenue
- Ohio Department Of Taxation
- Indiana Department Of Revenue
- Illinois Department Of Revenue
- Michigan Department Of Treasury

- Department Of Revenue
- Minnesota Revenue
- Department Of Revenue
- Missouri Department Of Revenue
- North Dakota Office Of State Tax Commissioner
- Nebraska Department Of Revenue
- Delaware Division Of Revenue
- Comptroller Of Maryland
- Office Of Tax And Revenue
- Virginia Department Of Taxation
- Tax And Revenue
- North Carolina Department Of Revenue
- South Carolina Department Of Revenue
- Georgia Department Of Revenue
- Kentucky Department Of Revenue
- Alabama Department Of Revenue
- Mississippi Department Of Revenue
- Bureau Of Internal Revenue
- Oklahoma Tax Commission
- Montana Department Of Revenue
- Idaho State Tax Commission
- Colorado Department Of Revenue
- New Mexico Taxation and Revenue Dept.
- Arizona Department Of Revenue
- Utah State Tax Commission
- Washington State Department Of Revenue
- Oregon Department Of Revenue
- Franchise Tax Board
- Dept. Of Labor & Industries
- Employment Development Department

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?
TPPS is unscheduled. A request for records disposition authority for TPPS and associated records is currently being drafted with the assistance of the IRS Records and Information Management (RIM) Program Office. When approved by the National Archives and Records Administration (NARA), disposition instructions for TPPS inputs, system data, outputs and system documentation will be published in IRM 1.15, exact Records Control Schedule and item number to be determined.

14. Will this system use technology in a new way?
No, the system does 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. This system will identify tax return preparers and can group them by their professional status and/or any other data element gathered at the time of application.

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.
Yes. The system does provide the capability to monitor individuals. The business purpose is to monitor tax preparer compliance through the registration process. Unauthorized access of the system by internal users is controlled through role–based access control (RBAC) and will be prevented through a combination of policy, education, and periodic checks to verify appropriate use of the information contained in the system.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?
No, the system does not allow taxpayers, employees, or others to be treated differently.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?
Yes, if the system captures data from the applicant that identifies a possible need for due process, then an alert will be sent to the IRS to take appropriate actions.

19. If the system is web–based, does it use persistent cookies or other tracking devices to identify web visitors?
The TPPS application is a web–based application. The application does not use persistent cookies or other tracking devices.

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