Trademark Processing System-Internal Systems (TPS-IS)
Privacy Threshold Analysis/ Privacy Impact Assessment (PTA/PIA)

Version 1.0

August 7, 2009

Prepared for:
Department of Commerce
United States Patent and Trademark Office
Office of Chief Information Officer
DOC50-PAPT-0905000

UNITED STATES PATENT AND TRADEMARK OFFICE

Record of Changes/Version History

PTA-PIA Template Version 6.2
October 1, 2008

Change/Version Number	Date of Change	Sections Changed	Description	Person Entering Change
Version 1.0	08/7/2009	All	Initial Version	Maria Sedlak

UNITED STATES PATENT AND TRADEMARK OFFICE

Privacy Threshold Analysis (PTA)

Instructions: Complete the "Privacy Threshold Analysis" section of this document and return it to United States Patent and Trademark Office (USPTO) Senior Privacy Official. If it is determined that a PIA is required as noted in the "Designation" section, the "Privacy Impact Assessment" section will be required to be completed and returned to the USPTO Senior Privacy Official for review and approval.

1. Describe the Trademark Processing System-Internal Systems (TPS-IS) and its purpose:

TPS-IS provides service support for processing trademark applications for the USPTO. TPS-IS includes 15 Automated Information Systems (AISs) that support internal users and managers through the trademark review process. The TPS features the ability to interface with related systems within USPTO.

TPS-IS is a Major System that consists of the following AISs:

1. First Action System for Trademarks 1 (FAST1)
2. First Action System for Trademarks 2 (FAST2)
3. Form Paragraph Editor Program (FPEP)
4. Fasteners Insignia Register System (FIRS)
5. Trademark Cropped Image Management (TCIM)
6. Trademark E-Commerce Law Offices (TECLO)
7. Trademark Image Capture and Retrieval System (TICRS)
8. Trademark In-house Photo Composition (TIPS)
9. Trademark Information System Reporting (TIS Reporting)
10. Trademark Postal System (TPostal)
11. Trademark Data Entry and Update System (TRADEUPS)
12. Trademark Reporting and Monitoring System (TRAM)
13. Trademark Reference Law Library System (TRLLS)
14. Trademark Search Facility-Design Search Code Automation (TSF-DSCA)
15. X-Search (XS)

2. Status of TPS-IS

☐ This is a new development effort.

☒ This is an existing system.

Date first developed: TPS has been a documented major application at USPTO since before 2006.

Date last updated: TPS was updated in 2008 for Certification and Accreditation (C&A) efforts. The addition of several components triggered the recertification of the system.

Current update: Currently, the legacy TPS is in the process of being split into two systems: TPS-ES (external-facing information systems) and TPS-IS (internal-facing information systems).

3. Does TPS-IS relate exclusively to the network infrastructure? [For example, is the system exclusively a Local Area Network (LAN) or Wide Area Network (WAN)]?

☒ No. Please continue to the next question.

☐ Yes. Is there a log kept of communication traffic?

☐ No. Please continue to the next question.

☐ Yes. What type of data is recorded in the log? (Please choose all that apply.)

☐ Header

☐ Payload

4. Could the TPS contain information that relates in any way to an individual?

☐ No. Please skip ahead to question 5.

☒ Yes. Please provide a general description, below.

TPS-IS applications, such as TEAS and TEASi, provide USPTO customers with the ability to submit trademark applications and register a trademark domestically and internationally, respectively. This information is stored within TRAM, a TPS-IS application.

5. Does TPS-IS use or collect Protectable Personally Identifiable Information (PII) [1] or Publicly Releasable PII[2]? (Refer to the USPTO IT Privacy Policy for additional information specific to handling PII.)

☐ No.

☒ Yes. TPS-IS stores Publicly Releasable PII.

Why does TPS-IS collect PII?

TPS-ES provides a means for registering, processing, and discovering trademarks. This publicly releasable PII collected by TPS-ES is stored within TRAM, which is within the TPS-IS accreditation boundary. The information is collected in order to transparently declare the ownership of a trademark.

6. What information about individuals could be collected, generated or retained?

Trademark registrants are required to provide the name of their entity (an individual or a business) and its street address. The registrant can also provide phone numbers and an email address.

[1] Protectable PII is defined as Information that can be used to uniquely identify (e.g., date of birth, gender, race, social security number, credit card account number, medical information, education information, etc.) contact (e.g., home address, phone number, etc.) or locate an individual (e.g., home or work address, etc).

[2] Publicly Releasable PII is defined as information identifiable to a specific individual that has been authorized for public release. The following information is publicly releasable PII:

- Non-financial information regarding business entities, such as business addresses, telephone numbers, web sites, e-mail; and
- Information available on the USPTO public website such as employee name, identification number, phone number and office location.

Designation

☐ This is NOT a Privacy Sensitive System – the system contains no PII.

☒ This IS a Privacy Sensitive System (Check all that apply)

- ☐ PTA sufficient at this time
- ☒ A PIA is required
- ☐ National Security System
- ☐ Legacy System
- ☐ HR System
- ☐ Financial System

I, as the system owner for the Trademark Processing System-Internal Systems (TPS-IS), concur with the information contained in this Privacy Threshold Analysis.

/s/ Glen Brown 8/26/2009

Glen Brown Date
System Owner for TPS-IS

I have reviewed this Privacy Threshold Analysis. I recommend that a Privacy Impact Assessment be completed.

/s/ Rod Turk 8/28/2009

Rod Turk Date
Senior Agency Information Security Officer for TPS-IS

I have reviewed, and approve this Privacy Threshold Analysis. A Privacy Impact Assessment is required.

/s/ John B. Owens II 9/3/2009

John B. Owens II Date
Co-Authorizing Official for TPS-IS

/s/ Lynne G. Beresford 1/2/2010

Lynne G. Beresford Date
Co-Authorizing Official for TPS-IS

cc: Deputy Chief Information Officer
Senior Agency Information Security Officer

Privacy Impact Assessment (PIA)

1. What information is to be collected (e.g., nature and source)?

Bibliographic information is required to be collected from trademark registrants, which includes:

a) The applicant's name and address

b) The applicant's legal entity;

The following information is collected from trademark registrants:

c) The citizenship of an individual applicant, or the state or country of incorporation or organization of a juristic applicant;

d) If the applicant is a partnership, the names and citizenship of the applicant's general partners;

e) A name and address for correspondence;

f) If applicant wants to correspond by e-mail or if applicant files application using TEAS-Plus, the system requires an e-mail address for correspondence, and an authorization for the Office to send e-mail correspondence concerning the application to the applicant or applicant's attorney.

2. Why is the information being collected (e.g., to determine eligibility)?

The information is collected to uniquely identify the applicant for trademark registration.

3. What is the intended use of the information (e.g., to verify existing data)?

The information becomes part of the official record of the application and is used to document registrant location and for official communications.

4. With whom will the information be shared (e.g., another agency for a specified programmatic purpose)?

During processing, the information is passed through to various internal AISs for processing at the USPTO. The information is not routinely shared with other agencies before publication; though the registrants can check on the progress of their applications.

After the application has been filed, the information is part of the public record. All information on Trademark files is available through TDR on the USPTO Web site.

5. What opportunities do individuals have to decline to provide information (where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how can individuals grant consent?

Individuals grant consent by filling out a trademark registration and submitting it for processing. A prominent warning on the TEAS system states

WARNING: All data you submit through TEAS will become public record and will be viewable in the USPTO's on-line databases, including your phone number, email address, and street address, where provided. Please avoid submitting personal identifying information that is NOT required for a filing, such as a social security number or driver's license number. Also, to maintain confidentiality of banking or credit card information, only enter payment information in the secure portion of the site after validating your form; do not enter a credit card number or other payment information anywhere within the front part of a TEAS form.

6. How will the information be secured (e.g., administrative and technological controls)?

Management Controls:

1. The USPTO uses the Life Cycle review process to ensure that management controls are in place for TPS-IS. During the enhancement of any component, the security controls are reviewed, re-evaluated, and updated in the Security Plan. The Security Plan specifically addresses the management, operational and technical controls that are in place and planned, during the operation of the enhanced system. Additional management controls include performing national agency check on all personnel, including contractor staff.

2. The USPTO Personally Identifiable Data Extracts Policy

Operational Controls:

1. Automated operational controls include securing all hardware associated with TPS-IS in the USPTO Data Center. The Data Center is controlled by access card entry, and is manned by a uniformed guard service to restrict access to the servers, their Operating Systems and databases. Contingency planning has been prepared for the data. Backups are performed on the processing databases. Backups are stored on tape and are secured off-site. Additional operation controls include: (1) Logical edit checks to ensure proper sequence of actions; (2) Physical terminal identification; (3) Database UserID; (4) Restricted data display, as required; and (5) Restricted access.
2. Manual procedures shall be followed for handling extracted data containing sensitive PII which is physically transported outside of the USPTO premises. In order to remove data extracts containing sensitive PII from USPTO premises, users must:
    a. Maintain a centralized office log for extracted datasets that contain sensitive PII. This log must include the date the data was extracted and removed from the

facilities, a description of the data extracted, the purpose of the extract, the expected date of disposal or return, and the actual date of return or deletion.

b. Ensure that any extract which is no longer needed is returned to USPTO premises or securely erased, and that this activity is recorded on the log.

c. Obtain management concurrence in the log, if an extract aged over 90 days is still required.

d. Store all PII data extracts maintained on an USPTO laptop in the encrypted My Documents directory. This includes any sensitive PII data extracts downloaded via the USPTO Virtual Private network (VPN).

e. Encrypt and password-protect all sensitive PII data extracts maintained on a portable storage device (such as CD, memory key, flash drive, etc.). Exceptions due to technical limitations must have the approval of the Office Director and alternative protective measures must be in place prior to removal from USPTO premises.

f. Encrypt and password-protect prior to transmission any sensitive PII data extracts that are sent to an external e-mail address via the Internet. The password key should be forwarded to the recipient in a separate e-mail from the attached file.

Technical Controls:

1. TPS-IS depends on NSI to provide a network of firewalls, Intrusion Detection Systems, and other devices to segregate publicly available information and services from sensitive internal information and services.

2. Access is controlled through a combination of Active Directory and updates to the TRAM database. Users are assigned to groups within Active Directory to gain access to certain shared folders but those permissions must also be manually entered into PALM, where they will propagate into the TRAM database every night. When a user attempts to authenticate to TRAM or any of its related applications, their Active Directory credentials are passed to TRAM, which checks its own tables to ensure the user should be granted access.

7. Is a system of records being created under the Privacy Act, 5 U.S.C. 552a?

According to the USPTO OCIO Records Officer and Legal Department, trademark data is not covered under the Privacy Act. Trademark information is inherently business, not personal; therefore a SORN is not required.

I, as the system owner for TPS-IS, concur with the information contained in this Privacy Impact Assessment.

/s/ Glen Brown 8/26/2009

Glen Brown Date
System Owner for TPS-IS

I have reviewed this Privacy Impact Assessment, and recommend it be approved.

/s/ Rod Turk 8/28/2009

Rod Turk Date
Senior Agency Information Security Officer for TPS-IS

I have reviewed, and approve this Privacy Impact Assessment.

/s/ John B. Owens II 9/3/2009

John B. Owens II Date
Co-Authorizing Official for TPS-IS

/s/ Lynne G. Beresford 1/2/2010

Lynne G. Beresford Date
Co-Authorizing Official for TPS-IS

cc: Deputy Chief Information Officer
Senior Agency Information Security Officer