U.S. DEPARTMENT OF COMMERCE

UNITES STATES PATENT AND TRADEMARK OFFICE

Privacy Impact Assessment

Trademark Processing System – Internal Systems

PTOT-003-00

March 24, 2015

Privacy Impact Assessment

This Privacy Impact Assessment (PIA) is a requirement of the Privacy Act of 1987 and OMB Memorandum 03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.* A PIA documents the due diligence and oversight placed upon information associated with the project or system in question. Written from the System Owner's perspective for the American public, the PIA discloses what information is being collected, and how that information is protected. The intent is to build confidence that privacy information is secure, processes that utilize this information comply with Federal requirements, and more importantly, inform the privacy expectations of the American public.

The Privacy Threshold Analysis (PTA) is a separate artifact that must be completed prior to beginning this PIA. In many cases, the PTA will be the only required artifact to satisfy DOC privacy considerations.

SYSTEM DESCRIPTION

The TPS-IS is a Major Application, and provides and provides support for the automated processing of trademark applications for the USPTO.

1. First Action System for Trademarks (FAST1)
2. First Action System for Trademarks 2 (FAST2)
3. Form Paragraph Editor Program (FPEP)
4. Trademark Cropped Image Manager (TCIM)
5. Trademark Image Capture and Retrieval System (TICRS)
6. Trademark In-house Photo Composition (TIPS)
7. Trademark Information System Reporting (TIS Reporting)
8. Trademark Postal System (TPostal)
9. Trademark Quality Review (TQRS)
10. Trademark Data Entry and Update System (TRADEUPS)
11. Trademark Reporting and Monitoring System (TRAM)
12. X-Search (XS)

QUESTIONNAIRE

1. What information is 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 this 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 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 (i.e., 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)?

In accordance with NIST 800-18 Rev. 1 and NIST 800-53 Rev. 4, the TPS-IS System Security Plan (SSP) addresses the extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment. The SSP is reviewed on an annual basis. In addition, annual assessments, Continuous Monitoring reviews, and triennial assessments are conducted. . The USPTO ITSMG conducts these assessments and reviews based on NIST SP 800-53 Revision 4, *Recommended Security Controls for Federal Information Systems* and NIST SP 800-53A Final *Guide for Assessing the Security Controls in Federal Information Systems*. The results of these assessments and reviews are documented in the TPS-IS Security Assessment Package as part of the system's Security Authorization process.

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. How will the data extract log and verify requirement be met?

   USPTO uses the following compensating controls to protect PII data:

   a. No extracts of sensitive data may be copied on to portable media without a waiver approved by the DoC CIO. The request for a waiver must include specifics as to how the data and device are protected, how long the data will be maintained, and how the data on the device will be deleted when no longer required.
   b. All laptop computers allowed to store sensitive data must have full disk encryption.
   c. All remote access to public USPTO systems containing sensitive data must be encrypted. All remote access to internal USPTO systems containing sensitive data must fully comply with DoC Remote Access Policy requirements.
   d. All flexi place/telework agreements for working off site require that adequate data protection be in place.

8. 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 Protectable Personally Identifiable Information[1]; it is Publicly Releasable PII[2]. Trademark information is inherently business, not personal; therefore a SORN is not required.

---

[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.

9. Are these records covered by a record control schedule approved by the National Archives and Records Administration (NARA)?

   No. GRC 20 allows agency determination that certain electronic records are authorized for erasure or deletion when they are no longer needed for administrative, legal, audit, or other operational purposes. Electronic records that represent hard copy records can be deleted after expiration of the retention period authorized for the hard copy records.

SIGNATORY AUTHORITY

Agreed: _____ 04 / 01 / 2015

Rajeev Dolas — Date

Information System Owner

Agreed: _____ 4 / 7 / 15

John Pardun — Date

Senior Information Security Officer

Agreed: _____ 4 / 8 / 15

John B. Owens II — Date

Authorizing Official