U.S. DEPARTMENT OF COMMERCE

UNITES STATES PATENT AND TRADEMARK OFFICE

Privacy Impact Assessment

Trademark Next Generation

PTOT-004-00

November 27, 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 TMNG is a Major Application, and provides support for the automated processing of trademark applications for the USPTO. It is comprised of the following 8 Automated Information Systems (AIS).

Authentication Authorization & Single Sign On (AASSO)

- Provide Single Sign On and role-based access

Trademark Status and Document Retrieval (TSDR)

- Will provide bibliographic data in a standard markup form.

Trademark Reporting and Data Mart (TRDM)

- Provide business reports and dashboards connecting to respective data sources.

Trademark Electronic Official Gazette (TMeOG)

- Enable consumers of published data in the official gazette to review information and search for items of interest.

Trademark Next Generation Identification Master List System (TMNG-IDM)

- Allows authorized users to perform editing functions (create, modify, delete), provide role-based, searching across current and archival versions.

TMNG Internal

- Used by Examining Attorneys during the Examination phase of an application.

Trademark Next Generation e-File (eFile)

- Used by customers to submit/make changes to Trademark Applications.

Trademark Next Generation Content Management System (TMNG_CMS)

- The purpose of TMNG_CMS is to transition to a single modern content repository that will be used by all TMNG internal systems.

TMNG is supported by the Trademark Next Generation Data Synchronization and Migration (DSM) tool, which acts as middleware between the TMNG applications and the legacy TRAM system, keeping data synchronized between the databases used by each system. Upon completion of the migration from the legacy Trademark systems to TMNG, the DSM tool will no longer be needed and will be removed.

QUESTIONNAIRE

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

   TSDR will make Trademark bibliographic data available to the public without the current data synchronization issues and will make TRAM bibliographic data available in a standard marked up form. This Trademark bibliographic data will also be available through a Web Service in addition to being available through the TSDR Web Page thus facilitating public access to Trademark data. TSDR uses name, address and phone number for contact purposes, which are all publicly available PII.

   eFile uses the Trademark case data stored in the TRM database for populating the Attorney forms. This data include the name of their entity (generally, a business) and its address. The registrant can also provide phone numbers and email address. The following information can be collected from trademark registrants, but it not required in order to submit the trademark for processing: if the applicant is a partnership, the names and citizenship of the applicant's general partners.

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

   The information collected by TSDR is to provide Trademark Application and Registration status and/or research access over the Internet to USPTO customers.

   The information in eFile is collected to uniquely identify the registrant of a trademark.

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

   The information in TSDR is used to communicate with the Public customers.

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

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

   The TSDR information is shared with members of the public.

   The eFile information is processed internally 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. A member of the public may request a copy of the application file.

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.

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 TMNG 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 and Continuous Monitoring reviews are conducted. The USPTO OPG-CD conducts these assessments and reviews based on NIST SP 800-53 Revision 4, S*ecurity and Privacy Controls for Federal Information Systems and*

Organizations 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 TMNG 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 TMNG. During the enhancement of any component, the security controls are reviewed, re-evaluated, and updated in the Security Plan. The Security Plans specifically address 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 checks on all personnel, including contractor staff.
2. A Security Categorization compliant with the FIPS 199 and NIST SP 800-60 requirements was conducted for TMNG. The overall FIPS 199 security impact level for TMNG was determined to be Moderate. This categorization influences the level of effort needed to protect the information managed and transmitted by the system.
3. The USPTO Personally Identifiable Data Removal Policy (see answer to Question 7 below).

Operational Controls:

1. Operational controls include securing all hardware associated with the TMNG 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.
2. Backups are managed by the Enterprise Tape Backup System (ETBS) and are secured off-site by First Federal.
3. Windows and Linux servers within TMNG are regularly updated with the latest security patches by the Enterprise Support Groups.
4. Additional operational controls include performing national agency checks on all personnel, including contractor staff.

Technical Controls:

1. TMNG 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 flexiplace/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.

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.

[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.

SIGNATORY AUTHORITY

Agreed: _____ 11 / 12 / 15

Jyotsna Jame — Date

Information System Owner

Agreed: _____ 11 / 18 / 15

John Pardun — Date

Senior Information Security Officer

Agreed: _____ 11 / 23 / 15

John B. Owens II — Date

Authorizing Official