

---

**U.S. DEPARTMENT OF COMMERCE**

**UNITED STATES PATENT AND TRADEMARK OFFICE**

---

**Privacy Impact Assessment**



**Trademark Processing System-External Systems (TPS-ES)**

**PTOT-002-00**

**February 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 components of TPS-ES are primarily located at 600 Dulany Street, Alexandria, VA 22314, on the 3<sup>rd</sup> floor, east wing at the Data Center. TPS-ES resides on the USPTO network (PTOnet).

TPS-ES provides service support for processing trademark applications for the USPTO.

TPS-ES includes seven applications that are used to support USPTO staff and public users through the trademark application process. TPS-ES features the ability to interface with related systems within USPTO, as well as with AISs outside USPTO.

TPS-ES is a Major Application (MA) comprising the following AISs:

1. Trademark Madrid System (MADRID)
2. Trademark Design and Search Code Manual (TDSCM)
3. Trademark Electronic Application System (TEAS)
4. Trademark Electronic Application System International (TEASi)
5. Trademark Electronic Search System (TESS)
6. Trademark Identification Manual (TIDM)

---

# QUESTIONNAIRE

---

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

Trademark registrants are required to provide the name of their entity (generally, a business) and its address. The registrant can also provide phone numbers and email address. This information can be queried from TRAM by several different publicly available search tools.

TEAS and TEASi applications provide USPTO customers with the ability to submit trademark applications and register a trademark domestically and internationally, respectively. This information is stored and is publically available for trademark discovery via TDSCM, TESS.

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

- a) The applicant's name and address
- b) The applicant's legal entity.

The following information can be collected from trademark registrants but it not required in order to submit the trademark for processing:

- c) If the applicant is a partnership, the names and citizenship of the applicant's general partners.
- d) The entity's address for correspondence
- e) An e-mail address for correspondence and an authorization for the Office to send correspondence concerning the application to the applicant or applicant's attorney by e-mail (only business email addresses are published).

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

The information 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 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. 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 filing out a trademark registration and submitting it for processing. A prominent warning on the TEAS system states:

### WARNINGS

**ALL DATA PUBLIC:** All information you submit to the USPTO at any point in the application and/or registration process will become public record, including your name, phone number, e-mail address, and street address. By filing this application, you acknowledge that **YOU HAVE NO RIGHT TO CONFIDENTIALITY** in the information disclosed. The public will be able to view this information in the USPTO's on-line databases and through Internet search engines and other on-line databases. This information will remain public even if the application is later abandoned or any resulting registration is surrendered, cancelled, or expired. To maintain confidentiality of banking or credit card information, only enter payment information in the secure portion of the site after validating your form. For any information that may be subject to copyright protection, by submitting it to the USPTO, the filer is representing that he or she has the authority to grant, and is granting, the USPTO permission to make the information available in its on-line database and in copies of the application or registration record.

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. 2 the TPS-ES 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 on TPS-ES data. The USPTO ITSMG conducts these assessments and reviews based on NIST SP 800-53 Revision 2, *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-ES Security Assessment Package as part of the system's Certification & Accreditation (C&A) process.

#### Management Controls:

1. The USPTO uses the Life Cycle review process to ensure that management controls are in place for TPS-ES. 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 TPS-ES. The overall FIPS 199 security impact level for TPS-ES 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 TPS-ES 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 TPS-ES are regularly updated with the latest security patches by the Unix System Support Groups.
4. Additional operational controls include performing national agency checks on all personnel, including contractor staff.

Technical Controls:

1. TPS-ES 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 implements the following practices to protect PII data:

No extracts of sensitive data may be copied onto 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.

All laptop computers allowed to store sensitive data must have full disk encryption.

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. 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<sup>1</sup>; it is Publicly Releasable PII<sup>2</sup>. Trademark information is inherently business, not personal; therefore a SORN is not required.

---

<sup>1</sup> 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).

<sup>2</sup> 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.

---

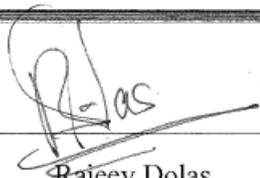
---

# SIGNATORY AUTHORITY

---

---

Agreed:



---

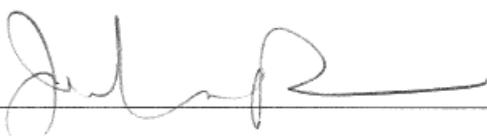
Rajeev Dolas

**Information System Owner**

02 / 02 / 2015

Date

Agreed:



---

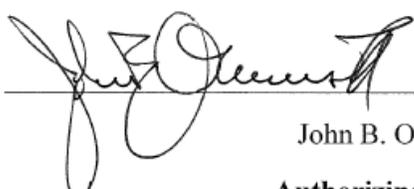
John Pardun

**Senior Information Security Officer**

3 / 10 / 2015

Date

Agreed:



---

John B. Owens II

**Authorizing Official**

3 / 11 / 15

Date