Version Number: 01-2019

U.S. Department of Commerce
U.S. Patent and Trademark Office

Privacy Threshold Analysis
for the
Trademark Processing System –External Systems

U.S. Department of Commerce Privacy Threshold Analysis

USPTO Trademark Processing System – External Systems

Unique Project Identifier: PTOT-002-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description of the information system in a way that a non-technical person can understand.*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

a) *Whether it is a general support system, major application, or other type of system*
Trademark Processing System - External Systems (TPS-ES) is a major application.

b) *System location*
The components of TPS-ES are primarily located at 600 Dulany Street, Alexandria, VA 22314, on the 3rd floor, east wing at the Data Center. TPS-ES resides on the USPTO network (PTOnet).

c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*
TPS-ES interconnects with Trademark Processing System – Internal Systems (TPS-IS).

d) *The purpose that the system is designed to serve*
TPS-ES provides support for the automated processing of trademark applications for the USPTO.

e) *The way the system operates to achieve the purpose*

Trademark Madrid System (MADRID) -The Madrid System assists the Office of Trademark in sending and receiving data from International Bureau (IB)-related to international applications that are being handled by the U.S. Patent and Trademark Office (USPTO).

Trademark Design and Search Code Manual (TDSCM) - TDSCM is a Web-based application

that allows trademark examining attorneys and the general public to search and retrieve design search codes from the TDSCM's Design Search Codes Manual.

Trademark Electronic Application System (TEAS)
Trademark Electronic Application System International (TEASi)
TEAS and TEASi provide customers with the means to electronically complete and register a trademark domestically or internationally. The applicant's information is stored and is publically available for trademark discovery via TDSCM and Trademark Electronic Search System. Bibliographic information collected from trademark registrants, include:

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

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

a. If the applicant is a partnership, the names and citizenship of the applicant's general partners.
b. The entity's address for correspondence.
c. 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).

The information is collected to uniquely identify the registrant of a trademark. The information becomes part of the official record of the application and is used to document registrant location and for official communications. After the application has been filed, the information is part of the public record and a member of the public may request a copy of the application file. However, applicants are informed and sign a consent that the information given will be accessible to the public. A prominent warning banner on TEAS 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.

Trademark Electronic Search System (TESS) - TESS is designed to provide the general public with the capability to search text and images of pending, registered, and dead Trademark applications via internet browser.

Trademark Identification Manual (TIDM) - The Trademark Identification Manual (TIDM)

system is a component that provides trademark examiners and the public with a web-based interface for searching and retrieving the text of the Trademark Classification Manual.

f) A general description of the type of information collected, maintained, use, or disseminated by the system

TPS-ES processes the following information types: Intellectual Property Protection information, Customer Services information, and Official Information Dissemination information.

g) Identify individuals who have access to information on the system

TPS-ES is accessible in whole or in part by the following: USPTO trademark business users, system administrators, system developers, and the general public.

h) How information in the system is retrieved by the user

TPS-ES uses web-based interfaces to access the information in the system. Some subsystems also provide web APIs to retrieve information in an automated fashion.

i) How information is transmitted to and from the system

TPS-ES uses HTTPS for transmitting to and from the system over the USPTO internal network, as well as the public internet.

Questionnaire:

1. What is the status of this information system?

☐ This is a new information system. *Continue to answer questions and complete certification.*

☐ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

☒ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

☐ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015).
Continue to answer questions and complete certification.

☐ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2017 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

☐ Yes. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

☒ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

☐ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

☐ Companies
☐ Other business entities

☒ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

☒ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

- ☐ DOC employees
- ☐ National Institute of Standards and Technology Associates
- ☐ Contractors working on behalf of DOC
- ☐ Other Federal Government personnel
- ☒ Members of the public

☐ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

☐ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
Provide the legal authority which permits the collection of SSNs, including truncated form.

☒ No, the IT system does not collect, maintain, or disseminate SSNs, user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

☒ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

☐ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

☐ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

☒ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

☒ I certify the criteria implied by one or more of the questions above **apply** to the Trademark Processing System - External Systems and as a consequence of this applicability, I will perform and document a PIA for this IT system.

☐ I certify the criteria implied by the questions above **do not apply** to the Trademark Processing System - External Systems and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (Acting) (SO): Ganesh Shetty

Signature of SO: Users, Shetty, Ganesh Digitally signed by Users, Shetty, Ganesh Date: 2020.04.13 07:09:59 -04'00' Date: _____

Name of Chief Information Security Officer (CISO): Don Watson

Signature of CISO: Users, Watson, Don Digitally signed by Users, Watson, Don Date: 2020.04.15 07:53:38 -04'00' Date: _____

Name of Authorizing Official (AO) & Bureau Chief Privacy Officer (BCPO): Henry J. Holcombe

Signature of AO & BCPO: Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry Date: 2020.04.21 07:13:38 -04'00' Date: _____