

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



**Privacy Impact Assessment
for the
Trademark Processing System – External Systems (TPS-ES)**

- ☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

CHARLES CUTSHALL

Digitally signed by CHARLES CUTSHALL
Date: 2025.02.04 10:40:36 -05'00'

2/4/2025

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Date

U.S. Department of Commerce Privacy Impact Assessment USPTO Trademark Processing System – External Systems (TPS-ES)

Unique Project Identifier: PTOT-002-00

Introduction: System Description

Provide a brief description of the information system.

Trademark Processing System – External Systems (TPS-ES) is a Major Application that provides customer support for processing Trademark applications for the United States Patent and Trademark Office (USPTO). TPS-ES includes four applications that are used to support USPTO staff and public users through the trademark application process. The four applications are described below:

MADRID Protocol is an international trademark filing and registration system that was designed to simplify and reduce the costs of foreign trademark filing. This protocol secures protection for the International Registration of Marks and is organized by the International Bureau (IB), a division of the World Intellectual Property Organization (WIPO).

Trademark Electronic Application System (TEAS) provides a web site for electronic filing of Trademark applications. post submission, TEAS facilitates the transfer of these applications to Trademark Operations for intake processing.

Trademark Electronic Application System International (TEASi) is a web application that provides users the ability to submit trademark applications that are filed under international treaties, satisfying the conditions and requirements of the MADRID Protocol Implementation Act and of the Office of Trademarks.

Address the following elements:

(a) Whether it is a general support system, major application, or other type of system

TPS-ES is a Major Application.

(b) System location

Manassas, VA

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

The TPS-ES is a Major Application that provides customer support for processing Trademark applications for USPTO. It interconnects with the following systems:

Fee Processing Next Generation (FPNG): allows internal and external users to manipulate payment accounts, perform profile updates, and make payments for USPTO goods and services.

Information Dissemination Support System (IDSS): is a major application that provides automated support for the timely search and retrieval of electronic text and images concerning patent applications and patents by USPTO internal and external users.

Intellectual Property Leadership Management System (IPLMSS): is a major application that groups and manages seven separate subsystems to provide tools to cull and organize large amounts of legal data to support the Freedom of Information Act (FOIA) requests, Privacy Act requests and appeals, to docket and track cases, manage library content, route electronic notices, develop and maintain assessments, and to register and maintain the practitioner roster and monitor practitioner disciplinary action.

MyUSPTO Cloud (MyUSPTO-C): reduces the number of logins for external USPTO customers and provides a single location from where they can conduct their business with the USPTO.

ICAM Identity as a Service (ICAM-IDaaS): provides an enterprise authentication and authorization service to all applications.

Enterprise Software Services (ESS): is a major application that provides an architecture capable of supporting current software services at USPTO.

Enterprise Desktop Platform (EDP): is an infrastructure information system that provides a standard enterprise-wide environment that manages desktops and laptops running on the Windows 7 and Windows 10 Operating System (OS).

Enterprise Windows Services (EWS): is an Infrastructure information system that provides a hosting platform for major applications that support various USPTO missions.

Network and Security Infrastructure System (NSI): is an Infrastructure information system and provides an aggregate of subsystems that facilitates the communications, secure access, protective services, and network infrastructure support for all USPTO Information Technology (IT) applications.

Security and Compliance Services (SCS): provides Security Incident and Event Management, Enterprise Forensic, Enterprise Management System, Security and Defense, Enterprise Scanner, Enterprise Cybersecurity Monitoring Operations, Performance Monitoring Tools, Dynamic Operational Support Plan, & Situational Awareness and Incident Response.

Storage Infrastructure Managed Services (SIMS): provides access to consolidated, block level data storage and files system storage. SIMS is primarily used to enhance storage devices, such as disk arrays, tape libraries, and optical jukeboxes.

Madrid International Trademark System (MITS): assists the Office of Trademark in sending, receiving, reviewing and verifying data from International Bureau (IB)-related to international applications that are being handled by the USPTO, as governed by the Madrid Protocol.

Trademark External (TM External): is comprised of different search components, Trademark External Filing (EFile), Trademark Status & Document Retrieval Services (TSDR), Trademark Pre-Examinations Application (TM-PEA), Trademark Electronic Official Gazette (TM-EOG), Trademark-Notification Services (TM-NS), Trademark Design Search Code Manual (TM-DSCM), Trademark Status Mobile Application (TSMA). Each of these components provide various means of locating trademark information.

Trademark Next Generation (TMNG): is a major application that provides support for the automated processing of trademark applications for the USPTO.

Trademark Processing System – Internal System (TPS-IS): is an information system that provides support for the automated processing of trademark applications for the USPTO.

Trilateral Network (TRINET): is an infrastructure information system, and provides secure network connectivity for electronic exchange and dissemination of sensitive patent data between authenticated endpoints at the Trilateral Offices and TRINET members. These Trilateral Offices include the USPTO as well as their counterparts in Europe and Japan. While the Korean Intellectual Property Office and the World Intellectual Property Office are TRINET members.

(d) The way the system operates to achieve the purpose(s) identified in Section 4

TPS-ES applications provide the following support for TPS-ES to achieve its purpose:

MADRID assists the Office of Trademark in sending and receiving data from IB-related to international applications that are being handled by the USPTO.

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 publicly available for trademark discovery via Trademark Electronic Search System (TESS). Bibliographic information collected from trademark registrants, include:

- The applicant's name and address.
- The applicant's legal entity.

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

- If the applicant is a partnership, the names and citizenship of the applicant's general partners.
- The entity's address for correspondence.
- An email address for correspondence and an authorization for the Office to send correspondence concerning the application to the applicant or applicant's attorney by email (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. Please see "Appendix A" for banner warning statement.

(e) How information in the system is retrieved by the user

TPS-ES uses web-based interfaces to access the information in the system. TPS-ES also uses web Application Programming Interfaces (APIs) to retrieve information in an automated fashion.

(f) How information is transmitted to and from the system

TPS-ES uses Hypertext Transfer Protocol Security (HTTPS) for transmitting to and from the system over the USPTO internal network, as well as the public internet.

(g) Any information sharing

TPS-ES shares trademark application data with Trademark Processing System – Internal Systems (TPS-IS), where the primary data repository resides.

TPS-ES shares international trademark data with IB, both sending and receiving internationally registered trademarks.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

5 U.S.C. § 301, 5 USC § 552, 44; U.S.C. § 3101; 35 U.S.C. § 2; 15 U.S.C. § 1051 et seq.; 37 CFR § 2.21.

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

The FIPS 199 security categorization for TPS-ES is Moderate.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

☐ This is a new information system.

☐ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions	<input type="checkbox"/>	d. Significant Merging	<input type="checkbox"/>	g. New Interagency Uses	<input type="checkbox"/>
b. Anonymous to Non-Anonymous	<input type="checkbox"/>	e. New Public Access	<input type="checkbox"/>	h. Internal Flow or Collection	<input type="checkbox"/>
c. Significant System Management Changes	<input type="checkbox"/>	f. Commercial Sources	<input type="checkbox"/>	i. Alteration in Character of Data	<input type="checkbox"/>
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.

☒ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

- 2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*	<input type="checkbox"/>	f. Driver's License	<input type="checkbox"/>	j. Financial Account	<input type="checkbox"/>
b. Taxpayer ID	<input type="checkbox"/>	g. Passport	<input type="checkbox"/>	k. Financial Transaction	<input type="checkbox"/>
c. Employer ID	<input type="checkbox"/>	h. Alien Registration	<input type="checkbox"/>	l. Vehicle Identifier	<input type="checkbox"/>
d. Employee ID	<input type="checkbox"/>	i. Credit Card	<input type="checkbox"/>	m. Medical Record	<input type="checkbox"/>
e. File/Case ID	<input type="checkbox"/>				
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	<input checked="" type="checkbox"/>	h. Date of Birth	<input type="checkbox"/>	o. Financial Information	<input type="checkbox"/>
b. Maiden Name	<input type="checkbox"/>	i. Place of Birth	<input type="checkbox"/>	p. Medical Information	<input type="checkbox"/>
c. Alias	<input type="checkbox"/>	j. Home Address	<input checked="" type="checkbox"/>	q. Military Service	<input type="checkbox"/>
d. Gender	<input type="checkbox"/>	k. Telephone Number	<input checked="" type="checkbox"/>	r. Criminal Record	<input type="checkbox"/>
e. Age	<input type="checkbox"/>	l. Email Address	<input checked="" type="checkbox"/>	s. Marital Status	<input type="checkbox"/>
f. Race/Ethnicity	<input type="checkbox"/>	m. Education	<input type="checkbox"/>	t. Mother's Maiden Name	<input type="checkbox"/>
g. Citizenship	<input checked="" type="checkbox"/>	n. Religion	<input type="checkbox"/>		
u. Other general personal data (specify): Citizenship is a standard asked question on the application.					

Work-Related Data (WRD)					
a. Occupation	<input type="checkbox"/>	e. Work Email Address	<input checked="" type="checkbox"/>	i. Business Associates	<input checked="" type="checkbox"/>
b. Job Title	<input type="checkbox"/>	f. Salary	<input type="checkbox"/>	j. Proprietary or Business Information	<input type="checkbox"/>
c. Work Address	<input checked="" type="checkbox"/>	g. Work History	<input type="checkbox"/>	k. Procurement/contracting records	<input type="checkbox"/>
d. Work Telephone Number	<input checked="" type="checkbox"/>	h. Employment Performance Ratings or other Performance Information	<input type="checkbox"/>		
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	<input type="checkbox"/>	f. Scars, Marks, Tattoos	<input type="checkbox"/>	k. Signatures	<input type="checkbox"/>

b. Palm Prints	<input type="checkbox"/>	g. Hair Color	<input type="checkbox"/>	l. Vascular Scans	<input type="checkbox"/>
c. Voice/Audio Recording	<input type="checkbox"/>	h. Eye Color	<input type="checkbox"/>	m. DNA Sample or Profile	<input type="checkbox"/>
d. Video Recording	<input type="checkbox"/>	i. Height	<input type="checkbox"/>	n. Retina/Iris Scans	<input type="checkbox"/>
e. Photographs	<input type="checkbox"/>	j. Weight	<input type="checkbox"/>	o. Dental Profile	<input type="checkbox"/>
p. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	<input checked="" type="checkbox"/>	c. Date/Time of Access	<input checked="" type="checkbox"/>	e. ID Files Accessed	<input type="checkbox"/>
b. IP Address	<input checked="" type="checkbox"/>	f. Queries Run	<input type="checkbox"/>	f. Contents of Files	<input type="checkbox"/>
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	<input type="checkbox"/>	Hard Copy: Mail/Fax	<input type="checkbox"/>	Online	<input checked="" type="checkbox"/>
Telephone	<input type="checkbox"/>	Email	<input type="checkbox"/>		
Other (specify):					

Government Sources					
Within the Bureau	<input checked="" type="checkbox"/>	Other DOC Bureaus	<input type="checkbox"/>	Other Federal Agencies	<input type="checkbox"/>
State, Local, Tribal	<input type="checkbox"/>	Foreign	<input checked="" type="checkbox"/>		
Other (specify):					

Non-government Sources					
Public Organizations	<input type="checkbox"/>	Private Sector	<input type="checkbox"/>	Commercial Data Brokers	<input type="checkbox"/>
Third Party Website or Application			<input type="checkbox"/>		
Other (specify): Attorney that represents a trademark filer					

2.3 Describe how the accuracy of the information in the system is ensured.

The information is provided directly by the individuals about whom the information pertains and they certify the accuracy of the information upon submission. Access controls, including the concept of least privilege, are in place within the system to protect the integrity of this data as it is processed or stored.

2.4 Is the information covered by the Paperwork Reduction Act?

<input checked="" type="checkbox"/>	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. 0651-0009 Applications for Trademark Registration 0651-0050 Response to Office Action & Voluntary Amendment Forms 0651-0051; Madrid Protocol 0651-0054: Substantive Submissions Made During the Prosecution of the Trademark Application 0651-0055: Post Registration 0651-0056: Submissions Regarding Correspondence and Regarding Attorney Representation 0651-0061: Trademarks Petitions
<input type="checkbox"/>	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards	<input type="checkbox"/>	Biometrics	<input type="checkbox"/>
Caller-ID	<input type="checkbox"/>	Personal Identity Verification (PIV) Cards	<input type="checkbox"/>
Other (specify):			

<input checked="" type="checkbox"/>	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.
-------------------------------------	--

Section 3: System Supported Activities3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings	<input type="checkbox"/>	Building entry readers	<input type="checkbox"/>
Video surveillance	<input type="checkbox"/>	Electronic purchase transactions	<input type="checkbox"/>
Other (specify): Click or tap here to enter text.			

<input checked="" type="checkbox"/>	There are not any IT system supported activities which raise privacy risks/concerns.
-------------------------------------	--

Section 4: Purpose of the System4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program	<input type="checkbox"/>	For administering human resources programs	<input type="checkbox"/>
For administrative matters	<input checked="" type="checkbox"/>	To promote information sharing initiatives	<input type="checkbox"/>
For litigation	<input type="checkbox"/>	For criminal law enforcement activities	<input type="checkbox"/>
For civil enforcement activities	<input type="checkbox"/>	For intelligence activities	<input type="checkbox"/>
To improve Federal services online	<input type="checkbox"/>	For employee or customer satisfaction	<input type="checkbox"/>
For web measurement and customization technologies (single-session)	<input type="checkbox"/>	For web measurement and customization technologies (multi-session)	<input type="checkbox"/>
Other (specify): To approve the trademark			

Section 5: Use of the Information

- 5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The bibliographic information stored in the system about applicants for a trademark is used to uniquely identify the registrant's trademark. Addresses and e-mail addresses are used for correspondence and as a means for the office to send correspondence concerning the application to the applicant or applicant's attorney. As anyone may register a trademark, the information may reference a federal employee, contractor, member of the public or a foreign national.

- 5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

The information is published to the public and submitters of information are made aware of this beforehand. Foreign entities, adversarial entities and insider threats are the threats to privacy within this system. Inadvertent private information exposure is a risk and USPTO has policies, procedures, and training to ensure that employees are aware of their responsibility of protecting sensitive information and the negative impact to the agency if there is a loss, misuse, or unauthorized access to or modification of sensitive private information. USPTO requires Annual Security Awareness Training for all employees as well as policies and procedures documented in the Cybersecurity Baseline Policy. All USPTO offices adhere to USPTO Records Management Office's Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citation.

Section 6: Information Sharing and Access

- 6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
DOC bureaus	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Federal agencies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
State, local, tribal gov't agencies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Private sector	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign governments	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign entities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other (specify): World Intellectual Property Organization (WIPO)	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

<input type="checkbox"/>	The PII/BII in the system will not be shared.
--------------------------	---

- 6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

<input type="checkbox"/>	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
<input checked="" type="checkbox"/>	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
<input type="checkbox"/>	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

- 6.3 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

<input checked="" type="checkbox"/>	<p>Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:</p> <p>FPNG IDSS IPLMSS MyUSPTO-C ICAM-IDaaS ESS TRINET TM-External SCS MITS TMNG TPS-IS</p>
-------------------------------------	--

	<p>During processing, the information is passed through to various internal information systems (see Introduction, question (c)) 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.</p> <p>The servers storing the potential PII are located in a highly sensitive zone within the USPTO internal network and logical access is segregated with network firewalls and switches through an Access Control list that limits access to only a few approved authorized accounts. USPTO monitors in real-time all activities and events within the servers storing the potential PII data and a subset of USPTO Cyber security personnel review audit logs received on a regular bases and alert the Information System Security Officer (ISSO) and/or the appropriate personnel when inappropriate or unusual activity is identified. Access is restricted on a “need to know” basis. Active Directory security groups are utilized to segregate users in accordance with their job functions.</p>
<input type="checkbox"/>	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public	<input checked="" type="checkbox"/>	Government Employees	<input checked="" type="checkbox"/>
Contractors	<input checked="" type="checkbox"/>		
Other (specify): Foreign entities			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

<input checked="" type="checkbox"/>	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
<input checked="" type="checkbox"/>	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://www.uspto.gov/privacy-policy	
<input checked="" type="checkbox"/>	Yes, notice is provided by other means.	Specify how: A notice is provided by a warning banner when the applicant accesses the application to submit a Trademark registration. In addition, a consent form is signed by the applicant giving USPTO the authority to share the information provided with the public. Please see “Appendix A” for details on warning banner.
<input type="checkbox"/>	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

<input type="checkbox"/>	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: The information collected is required for trademark registration and processing. Individuals are notified that the information that they submit will become public information. If individuals decline to provide PII then USPTO cannot submit a trademark for registration for processing.

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

<input type="checkbox"/>	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: The individuals do not have the opportunity to consent to particular uses of their PII/BII. The information collected is required for trademark registration and processing. Individuals are notified that the information that they submit will become public information.

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

<input type="checkbox"/>	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how:
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: Individuals cannot review or update the PII/BII within TPS-ES however the individuals can work with USPTO if their contact information needs to be review or updated.

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

<input type="checkbox"/>	All users signed a confidentiality agreement or non-disclosure agreement.
<input type="checkbox"/>	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
<input checked="" type="checkbox"/>	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
<input checked="" type="checkbox"/>	Access to the PII/BII is restricted to authorized personnel only.
<input checked="" type="checkbox"/>	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Audit Logs
<input checked="" type="checkbox"/>	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 2/29/2024

<input type="checkbox"/>	This is a new system. The A&A date will be provided when the A&A package is approved.
<input checked="" type="checkbox"/>	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
<input checked="" type="checkbox"/>	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 5 recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
<input checked="" type="checkbox"/>	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
<input checked="" type="checkbox"/>	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
<input type="checkbox"/>	Contracts with customers establish DOC ownership rights over data including PII/BII.
<input checked="" type="checkbox"/>	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
<input type="checkbox"/>	Other (specify):

- 8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

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 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 checks on all personnel, including contractor staff. A Security Categorization compliant with the Federal Information Processing Standards (FIPS) 199 and National Institute of Standards and Technology (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. Operational controls include securing all hardware associated with the TPS-ES in the USPTO Data Center. The Data Center is controlled by a access card entry and is manned by a uniformed guard service to restrict access to the servers, their operating systems, and databases. Application servers within TPS-ES are regularly updated with the latest security patches by the Operational Support Groups. Additional operational controls include performing national agency checks on all personnel, including contractor staff.

Section 9: Privacy Act

- 9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

- ☒ Yes, the PII/BII is searchable by a personal identifier.
- ☐ No, the PII/BII is not searchable by a personal identifier.

- 9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

<input checked="" type="checkbox"/>	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. <i>(list all that apply):</i> COMMERCE/PAT-TM-23 : User Access for Web Portals and Information Requests COMMERCE/PAT-TM-26 : Trademark Application and Registration Records
<input type="checkbox"/>	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
<input type="checkbox"/>	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

<input checked="" type="checkbox"/>	There is an approved record control schedule. Provide the name of the record control schedule: N1-241-05-2:5: Information Dissemination Product Reference N1-241-06-2:2: Trademark Case File Feeder Records and Related Indexes, selected N1-241-06-2:3: Trademark Case File Feeder Records and Related Indexes, non-selected N1-241-06-2:4: Trademark Case File Feeder Records and Related Indexes N1-241-06-2:5: Trademark Routine Subject Files
<input type="checkbox"/>	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
<input checked="" type="checkbox"/>	Yes, retention is monitored for compliance to the schedule.
<input type="checkbox"/>	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	<input type="checkbox"/>	Overwriting	<input type="checkbox"/>
Degaussing	<input type="checkbox"/>	Deleting	<input checked="" type="checkbox"/>
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII*

Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)

<input checked="" type="checkbox"/>	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
<input type="checkbox"/>	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
<input type="checkbox"/>	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact level.
(Check all that apply.)

<input checked="" type="checkbox"/>	Identifiability	Provide explanation: Name, Home address, Telephone number, email address, work address, work email address, and work phone number together can identify a particular individual.
<input checked="" type="checkbox"/>	Quantity of PII	Provide explanation: The PII is publicly available and varies depending on the number of applications.
<input checked="" type="checkbox"/>	Data Field Sensitivity	Provide explanation: The data includes limited personal and work-related elements, and does not include sensitive identifiable information since all the information processed by TPS-ES is public record information.
<input checked="" type="checkbox"/>	Context of Use	Provide explanation: The personally identifiable information processed by TPS-ES is used to identify the individuals or companies that have registered trademarks with the government of the United States.
<input checked="" type="checkbox"/>	Obligation to Protect Confidentiality	Provide explanation: There is no obligation to protect the confidentiality of the personally identifiable information; the PII processed by TPS-ES is public record information.
<input checked="" type="checkbox"/>	Access to and Location of PII	Provide explanation: The PII on this system is available to the general public through the patent website.
<input type="checkbox"/>	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

The threats to the sensitive PII in the system are insider threats and foreign entities. The non-sensitive information in the system can be retrieved by the public. USPTO implements security and management controls to prevent the inappropriate disclosure of sensitive information. Security controls are employed to ensure information is resistant to tampering, remains confidential as necessary, and is available as intended by the Agency and as expected by authorized users. Management controls are utilized to prevent the inappropriate disclosure of sensitive information. NSI and SCS provide additional automated transmission and monitoring mechanisms to ensure that PII/BII information is protected and not breached by external entities.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

<input type="checkbox"/>	Yes, the conduct of this PIA results in required business process changes. Explanation:
<input checked="" type="checkbox"/>	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

<input type="checkbox"/>	Yes, the conduct of this PIA results in required technology changes. Explanation:
<input checked="" type="checkbox"/>	No, the conduct of this PIA does not result in any required technology changes.

Appendix A



This is a government computer system and is intended for official and other authorized use only. Unauthorized access or use of the system is prohibited and subject to administrative action, civil, and criminal prosecution under 18 USC 1030. All data contained on this information system may be monitored, intercepted, recorded, read, copied, or captured and disclosed by and to authorized personnel for official purposes, including criminal prosecution. You have no expectations of privacy regarding monitoring of this system. Any use of this computer system signifies consent to monitoring and recording, and compliance with USPTO policies and their terms.