

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



**Privacy Impact Assessment
for the
Trademark Processing System – Internal System (TPS-IS)**

Reviewed by: Henry J. Holcombe, Bureau Chief Privacy Officer

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

JENNIFER GOODE Digitally signed by JENNIFER GOODE
Date: 2021.08.19 16:57:03 -04'00'

08/11/2021

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

Date

U.S. Department of Commerce Privacy Impact Assessment USPTO Trademark Processing System – Internal System (TPS-IS)

Unique Project Identifier: PTOT-003-00

Introduction: System Description

Provide a description of the system that addresses the following elements:

The response must be written in plain language and be as comprehensive as necessary to describe the system.

The TPS-IS is an Application information system that provides support for the automated processing of trademark applications for the USPTO. TPS-IS includes ten applications that are used to support USPTO staff through the trademark review process. TPS-IS features the ability to interface with related systems within USPTO.

TPS-IS is comprised of the following AISs:

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 Information System Reporting -TIS Reporting
7. Trademark Postal System - TPostal
8. Trademark Data Entry and Update System - TRADEUPS
9. Trademark Reporting and Monitoring System - TRAM
10. X-Search - XS

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

Trademark Processing System – Internal Systems (TPS-IS) is a major application.

(b) System location

The components of TPS-IS are primarily located at the United States Patent and Trademark Office (USPTO) Data Center at 600 Dulany Street, Alexandria, Virginia. TPS-IS 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-IS interconnects with Trademark Processing System – External Systems (TPS-ES) and Trademark Next Generation (TMNG). **TPS-ES** is major application information system, and provides customer support for processing Trademark applications for USPTO. **TMNG** is a

major application and provides support for the automated processing of trademark applications for the USPTO.

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

TPS-IS includes 10 applications that are used to support USPTO staff through the trademark review process. TPS-IS features the ability to interface with related systems within USPTO. TPS-IS is comprised of the following Automated Information Systems (AISs):

First Action System for Trademarks 1 (FAST1): FAST1 provides an automated system as a front-end tool that gives examiners the ability to electronically examine new trademark applications without the need of a paper application. This system also provides examiners with application functions that perform first and subsequent office actions, create validation reports, and manage dockets. It processes the PII data collected by the Trademark Processing System-External Systems (TPS-ES) as part of the trademark application process.

First Action System for Trademarks 2 (FAST2): FAST2 serves the USPTO Trademark Legal Instruments Examiner (LIE), their supervisors (SLIE), and the Intent to Use (ITU) staff. LIEs are personnel that perform reviews and update trademark cases. Each LIE is assigned to a law office where a system is needed to aid them in processing the work item associated with trademark cases. The FAST2 system allows LIEs to process the work items assigned to them. FAST2 presents the LIEs with a list of work items and allows them to choose items to process. When processing a work item, the FAST2 system allows the user to view and/or edit case information in related systems. It processes the PII data collected by TPS-ES as part of the trademark application process.

Form Paragraph Editor Program (FPEP): FPEP enables form paragraph editors to manage form paragraph data. Using FPEP, editors are able to create, delete, modify, and publish form paragraphs, and produce reports. Published form paragraphs are available to Trademark examiners through a presentation layer in FAST1 and FAST2. It does not process PII data.

Trademark Cropped Image Management (TCIM): TCIM accepts cropped images from Trademark Electronic Application System (TEAS), the Trademark Data Entry and Update System (TRADEUPS), and the Data Management Branch of the Office of System Network Management. The images are stored in a directory structure based on the serial number of the associated trademark application. The TCIM database keeps an inventory of the stored image files and the date each file was received. It does not process PII data.

Trademark Image Capture and Retrieval System (TICRS): TICRS is designed to capture, store, retrieve, and print digital images of trademark application documents. TICRS has the following logical components: (1) the capture component enables the input of digital images by

scanning paper and the capture of index data; (2) the storage component manages the physical storage of images and provides access control to maintain security; and (3) the retrieval component provides query and output capabilities for applications within the system. The information in the system is exported to a PDF document and given to the USPTO Webmaster to post onto the USPTO public website. Through USPTO's website, the general public is able to query the PDF document to determine active fastener insignias. It processes the PII data collected by TPS-ES as part of the trademark application process.

Trademark Information System Reporting (TIS Reporting): TIS Reporting provides enhanced reporting capabilities that are flexible and accessible to Trademark Management. The system enables the design, scheduling, running, and web-based distribution of management reports. TIS Reporting facilitates the capability to view, print, and export reports to common file formats, all from the end-user workstation. It does not process PII data.

Trademark Postal System (TPostal): TPostal serves trademark notices to trademark applicants, replacing the manual system for the production of most trademark outgoing notices. USPTO uses an automatic postcard services provided by the Click2Mail system. Click2Mail is a partner of the U.S. Postal Service that supports electronic submission of notices to be mailed. TPostal implements the necessary interface to Click2Mail. TPostal generates and sends bulk mail to the Click2Mail website for printing, stamping, and mailing trademark notices; no user intervention is required. It processes the PII data collected by TPS-ES as part of the trademark application process.

Trademark Data Entry and Update System (TRADEUPS): TRADEUPS is used for new application data entry and the editing of bibliographic data and Trademark text. The system is designed to interface with the TRAM System and the USPS address verification software to verify that the correspondence address submitted by an applicant is deliverable. TRADEUPS includes those data elements and functions required to process new applications in the Pre-Examination Section. It processes the PII data collected by TPS-ES as part of the trademark application process.

Trademark Reporting and Monitoring System (TRAM): TRAM provides support to all facets of trademark operations. TRAM includes a database consisting of bibliographic text and prosecution history data. TRAM also supports trademark operations from receipt of new applications to the publication of the TMOG and post-registration activities. The publicly-releasable PII collected by components of the Trademark Processing System-External Systems (TPS-ES) system is stored within TRAM.

X-Search (XS): XS is a client-server application that supports Trademark Examination attorneys searching for existing marks prior to granting a registration. The application's GUI

allows users to perform searches, display hit lists, and print and save search histories; displays associated cropped images; and provides online help. It also provides access to reference materials for use by the trademark examiners and lawyers. It is used to support the information needs of the Trademark Examining Attorneys. It processes the PII data collected by TPS-ES as part of the trademark application process.

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

TPS-IS uses client/server and web-based interfaces to access the information in the system.

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

TPS-IS uses HTTP for transmitting to and from the system over the USPTO internal network. All data in transit is encrypted and all requests that are made will automatically be re-directed to HTTPS.

(g) Any information sharing conducted by the system

TPS-IS shares trademark application data with USPTO's Trademark Processing System – External Systems (TPS-ES) and Trademark Next Generation (TMNG) and the public via the TRAM database. The bureau intends to share the PII in the IT system within the bureau via direct access and give the public access to the non-sensitive PII in the system on a case-by-case basis.

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

35 U.S.C. § 2; 15 U.S. C. § Chapter 22; 37 CFR § 2.

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

The FIPS 199 security categorization for TPS-IS 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 (version 01-2015 or 01-2017).
- ☐ 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 01-2019 or later).

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 checked="" 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. Physical Characteristics	<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):					

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 checked="" type="checkbox"/>	f. Salary	<input type="checkbox"/>	j. Proprietary or Business Information	<input checked="" 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 type="checkbox"/>	c. Date/Time of Access	<input 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 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):

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

<p>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, stored, and dispositioned. 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 PII.</p>

2.4 Is the information covered by the Paperwork Reduction Act?

<input checked="" type="checkbox"/>	<p>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 0651-0027: Recording Assignments 0651-0028: Fastener Quality Act Insignia Record Process 0651-0048: Native American Tribal Insignia 0651-0050: Response to Office Action and 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</p>
<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 Activities**3.1 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):			

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

Section 4: Purpose of the System

4.1 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 checked="" 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 checked="" 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):			

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).

<p>The information about applicants that are stored in the system are about members of the public. USPTO employees and contractors working in the system also have their names in the system. Addresses and e-mail addresses are used for correspondence and as authorization for the Office to send correspondence concerning the application to the applicant or applicant's attorney. The system collects trademark application data such as the applicant's name and address, and legal entity such as a corporation, partnership, LLC, etc.</p>
--

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 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 on a case-by-case basis. 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. The Perimeter Network and Security Infrastructure (NSI) and Enterprise Monitoring and Security Operations (SCS) provide additional automated transmission and monitoring mechanisms to ensure that PII/BII information is protected and not breached by external entities.

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 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):	<input type="checkbox"/>	<input 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>All user access is governed by a role based and need-to-know basis that is either Active Directory or Role Base Access Control (RBAC) enforced. The TRAM component of TPS-IS is used to store the records collected by TPS-ES components. The TRAM component synchronizes its stored records with the TMNG system, so examination of applications can occur using TMNG as well as TPS-IS. TPS-IS implements secure network communications are via end-to-end transport layer protocols and where applicable data-at-rest encryption. The information transmitted between the systems is protected within USPTO's secure perimeter through the NSI and SCS systems</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 type="checkbox"/>	Government Employees	<input checked="" type="checkbox"/>
Contractors	<input checked="" type="checkbox"/>		
Other (specify):			

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 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:	
<input checked="" type="checkbox"/>	Yes, notice is provided by other means.	Specify how: A notice is provided by a warning banner when the employee or contractor logs into the workstation before accessing the TPS-IS system. See banner in APPENDIX A .
<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 checked="" 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: Individuals grant consent by filling out a trademark registration and submitting it for processing. They are notified that some of the information that they submit will become public information. They may decline to provide PII by not submitting a trademark 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: Consent is given at the front end systems.

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: The opportunity to review/update PII/BII is given at the front end systems.

Section 8: Administrative and Technological Controls

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

<input checked="" type="checkbox"/>	All users signed a confidentiality agreement or non-disclosure agreement.
<input checked="" 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): <u>June 10, 2021</u> <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 4 Appendix J 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 checked="" 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-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 background checks on all personnel, including contractor staff.

A Security Categorization compliant with the FIPS 199 and NIST SP 800-60 requirements was conducted for TPS-IS. The overall FIPS 199 security impact level for TPS-IS 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-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. Backups are managed by the Enterprise Tape Backup System (ETBS) and are secured off-site by First Federal. Application servers within TPS-IS are regularly updated with the latest security patches by the Operational Support Groups.

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/USPTO-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: N1-241-06-2:2: Trademark Case File Records and Related Indexes, selected N1-241-06-2:3: Trademark Case File Records and Related Indexes, non-selected N1-241-06-2:4: Trademark Case File Feeder Records and Related Indexes N1-241-06-2:5: Trademarks Routine Subject Files GRS 5.1, item 020: Non-Recordkeeping Copies of Electronic Records GRS 5.2, item 020: Intermediary Records N1-241-05-2:5: Information Dissemination Product Reference
<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 checked="" 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 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 checked="" 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: The combination of name, home address, citizenship, email address, job title, etc., can easily identify a particular person.
<input checked="" type="checkbox"/>	Quantity of PII	Provide explanation: The quantity of PII contained in this system is large enough to require adequate protection.
<input checked="" type="checkbox"/>	Data Field Sensitivity	Provide explanation: The PII data fields when combined would have an adverse effect on the organization or individuals if a loss were to occur.
<input checked="" type="checkbox"/>	Context of Use	Provide explanation: The personally identifiable information processed by TPS-IS 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: Based on the data fields and in accordance with the Privacy Act of 1974, PII must be protected. The sensitive PII in the system needs certain security and privacy controls. Sensitive information found in the system is protected through access control and Disk Level encryption.
<input checked="" type="checkbox"/>	Access to and Location of PII	Provide explanation: Government employees and contractors will have direct access to the PII. Access is limited only to the identified and authenticated users and partners.
<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 on a case-by-case basis. 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

*****WARNING*****WARNING*****WARNING*****

You have accessed a United States Government computer system. Unauthorized access or actions exceeding authorized access is a violation of Public Law 99-474; 18 U.S.C. 1030 and may result in criminal, civil or administrative penalties. Authorized use of this system is limited to work needed to perform official US Patent and Trademark Office (USPTO) business. While using this system, users must comply with USPTO policy as documented in the USPTO AAO 212-4, Information Technology Security. Unauthorized use, or modification or disclosure of the data contained herein or in transit to/from this system constitutes a violation of Public Law 99-474; 18 U.S.C. 1030 and state criminal and civil laws. Users of this system may be monitored in order to ensure its continued operational effectiveness and integrity. Users of this system are reminded that such monitoring does occur and that use of this system constitutes consent to such monitoring. Unauthorized use or actions exceeding authorized use of USPTO systems will be investigated and, when appropriate, official sanctions will be imposed. If criminal activity is discovered, systems information will be provided to the appropriate law enforcement officials for investigation and prosecution. Report access violations or policy infractions to the Service Desk at (571) 272-9000.

*****WARNING*****WARNING*****WARNING*****