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

Privacy Impact Assessment
for the
Trademark Processing System – Internal Systems

Reviewed by: Henry J. Holcombe Jr., 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

KRISTEN LEFEVRE Digitally signed by KRISTEN LEFEVRE
Date: 2019.06.05 18:17:42 -04'00'

for Dr. Catrina D. Purvis   06/05/2019

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 Systems

Unique Project Identifier: PTOT-003-00

<u>Introduction</u>: System Description

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

(a) a general description of the information in the system

The components of Trademark Processing System – Internal Systems (TPS-IS) are primarily located at the USPTO Data Center in Alexandria, Virginia. TPS-IS resides on the USPTO network (PTOnet).

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 (AIS):

1. 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.

2. 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.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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 service provided by the Click2Mail system. Click2Mail is a partner of the US 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.

8. 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.

9. 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.

10. 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.

(b) a description of a typical transaction conducted on the system

Trademark examiners use the FAST1 system to access the applications that have been assigned to them. FAST1 retrieves the application data from the TRAM system. The examiner processes the application, using X-Search to research potentially conflicting marks, and determines if the registration should be granted or denied. Notices of registration, whether processed by examiners using TPS-IS or Trademark Next Generation (TMNG), are sent via TPostal.

(c) any information sharing conducted by the system

TPS-IS receives trademark application data from Trademark Processing System – External Systems (TPS-ES) and stores it in the TRAM AIS. It also provides data to TPS-ES for display of public trademark information as well as to allow applicants to update trademark applications or registration information.

TPS-IS shares trademark data with the TMNG system. Data is synchronized between TRAM and TMNG, allowing trademark examiners to conduct their examinations using TMNG.

(d) a citation of the legal authority to collect PII and/or BII

35 U.S.C. § 2; 15 U.S. Code § 1051 *et seq.*; 37 CFR § 2.21.

(e) the Federal Information Processing Standard (FIPS) 199 security impact category for the system

The Federal Information Processing Standard (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.)*

☒   This is an existing information system in which changes do not create new privacy risks. *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):					

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*	☐	e. File/Case ID	☐	i. Credit Card	☐
b. Taxpayer ID	☐	f. Driver's License	☐	j. Financial Account	☐
c. Employer ID	☐	g. Passport	☐	k. Financial Transaction	☐
d. Employee ID	☐	h. Alien Registration	☐	l. Vehicle Identifier	☐
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					
*If SSNs are collected, stored, or processed by the system, please explain if there is a way to avoid such collection in the future and how this could be accomplished:					

General Personal Data (GPD)					
a. Name	☒	g. Date of Birth	☐	m. Religion	☐
b. Maiden Name	☐	h. Place of Birth	☐	n. Financial Information	☐
c. Alias	☐	i. Home Address	☒	o. Medical Information	☐

d. Gender	☐	j. Telephone Number	☒	p. Military Service	☐
e. Age	☐	k. Email Address	☒	q. Physical Characteristics	☐
f. Race/Ethnicity	☐	l. Education	☐	r. Mother's Maiden Name	☐
s. Other general personal data (specify): Country of Citizenship, Fax Number					

Work-Related Data (WRD)					
a. Occupation	☐	d. Telephone Number	☒	g. Salary	☐
b. Job Title	☐	e. Email Address	☒	h. Work History	☐
c. Work Address	☒	f. Business Associates	☒		
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	☐	d. Photographs	☐	g. DNA Profiles	☐
b. Palm Prints	☐	e. Scars, Marks, Tattoos	☐	h. Retina/Iris Scans	☐
c. Voice Recording/Signatures	☐	f. Vascular Scan	☐	i. Dental Profile	☐
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	☐	c. Date/Time of Access	☐	e. ID Files Accessed	☐
b. IP Address	☐	d. Queries Run	☐	f. Contents of Files	☐
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	☐	Hard Copy: Mail/Fax	☒	Online	☒
Telephone	☐	Email	☐		
Other (specify):					

Government Sources					
Within the Bureau	☐	Other DOC Bureaus	☐	Other Federal Agencies	☐
State, Local, Tribal	☐	Foreign	☐		
Other (specify):					

Non-government Sources					
Public Organizations	☐	Private Sector	☐	Commercial Data Brokers	☐
Third Party Website or Application			☐		

Other (specify):

2.3   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	☐	Biometrics	☐
Caller-ID	☐	Personal Identity Verification (PIV) Cards	☐
Other (specify):			

☒	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	☐	Building entry readers	☐
Video surveillance	☐	Electronic purchase transactions	☐
Other (specify):			

☒	There are not any IT system 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			
To determine eligibility	☐	For administering human resources programs	☐
For administrative matters	☒	To promote information sharing initiatives	☐
For litigation	☐	For criminal law enforcement activities	☐
For civil enforcement activities	☐	For intelligence activities	☐
To improve Federal services online	☐	For employee or customer satisfaction	☐
For web measurement and customization technologies (single-session)	☐	For web measurement and customization technologies (multi-session)	☐
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).

The bibliographic information stored in the system about applicants for a trademark are used to uniquely identify the registrant trademark. Addresses and e-mail addresses are used for correspondence and an authorization for the Office to send correspondence concerning the application to the applicant or applicant's attorney (only business email addresses are published).

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	☐	☐	☒
DOC bureaus	☐	☐	☐
Federal agencies	☐	☐	☐
State, local, tribal gov't agencies	☐	☐	☐
Public	☒	☐	☒
Private sector	☐	☐	☐
Foreign governments	☐	☐	☐
Foreign entities	☐	☐	☐
Other (specify):	☐	☐	☐

☐	The PII/BII in the system will not be shared.

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

⊠	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: 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.
☐	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3   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	⊠	Government Employees	⊠
Contractors	⊠		
Other (specify): The general public will not have direct access to the IT system, but will have access to the PII stored within the system through the public-facing components of the TPS-ES system.			

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.)*

⊠	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.
☐	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: _____.
⊠	Yes, notice is provided by other means.	Specify how: A notice is provided by a warning banner when the applicant accesses the TPS-ES system where they provide the data that is stored by the TRAM component of TPS-IS. In addition a consent form is signed by the applicant giving USPTO the authority to share the information provided with the public. The warning banner presented 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.
☐	No, notice is not provided.	Specify why not:

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

☒	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Individuals grant consent by filing out a trademark registration and submitting it for processing. They are notified that the information that they submit will become public information. They may decline to provide PII by not submitting a trademark registration for processing.
☐	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

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

☒	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: All information collected is for contact purposes. Individuals have a choice of what contact information to give. They are also made aware that the information provided will be made public.
☐	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

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

☒	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Individuals will need to work with USPTO if contact information changes to update their records.
☐	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

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

☐	All users signed a confidentiality agreement or non-disclosure agreement.
☐	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
☒	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
☐	Access to the PII/BII is restricted to authorized personnel only.
☐	Access to the PII/BII is being monitored, tracked, or recorded. Explanation:
☒	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): __June 9, 2018_____ ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
☒	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
☒	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 (POAM).
☐	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
☐	Contracts with customers establish ownership rights over data including PII/BII.
☒	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
☐	Other (specify):

8.2   Provide a general description of the technologies used to protect PII/BII on the IT system.

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 national agency 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.

Application servers within TPS-IS 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 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."

☒	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: COMMERCE/DEPT 23 SORN
☐	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u>.
☐	No, a SORN is not being created.

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.)*

☒	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
☐	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:
☒	Yes, retention is monitored for compliance to the schedule.
☐	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	☒	Overwriting	☐
Degaussing	☒	Deleting	☒
Other (specify):			

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

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.

☒	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
☐	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
☐	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 levels. *(Check all that apply.)*

☐	Identifiability	Provide explanation:
☐	Quantity of PII	Provide explanation:
☒	Data Field Sensitivity	Provide explanation: The personally identifiable information processed by TPS-IS is public record information.
☒	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.
☐	Obligation to Protect Confidentiality	Provide explanation:
☐	Access to and Location of PII	Provide explanation:
☐	Other:	Provide explanation:

Section 12: Analysis

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

☐	Yes, the conduct of this PIA results in required business process changes. Explanation:
☒	No, the conduct of this PIA does not result in any required business process changes.

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

☐	Yes, the conduct of this PIA results in required technology changes. Explanation:
☒	No, the conduct of this PIA does not result in any required technology changes.