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

Privacy Impact Assessment
for the
Trademark Next Generation

Reviewed by: David Chiles, Bureau Chief Privacy Officer (Acting)

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

CATRINA PURVIS

Digitally signed by CATRINA PURVIS
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the
Secretary, cn=CATRINA PURVIS, 0.9.2342.19200300.100.1.1=13001002875743
Date: 2019.02.08 18:08:10 -05'00'

11/21/2018

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO Trademark Next Generation

Unique Project Identifier: PTOT-004-00

Introduction: 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 Next Generation (TMNG) are primarily located at 600 Dulany Street, Alexandria, VA 22314, on the 3rd floor, east wing at the Data Center. TMNG resides on the USPTO network (PTOnet).

TMNG includes eight automated information systems (AIS), which provide support for the automated processing of trademark applications for the USPTO. TMNG features the ability to interface with related systems within USPTO.

TMNG is comprised of the following AISs:

Authentication Authorization & Single Sign On (AASSO)
> AASSO provides Single Sign On and role-based access to the other components of TMNG.

Trademark Status and Document Retrieval (TSDR)
> The TSDR web application enables users to perform research and/or investigate specific trademarks information and documents. The application has four categories of users: Public Users, Public Data Miner Users, internal USPTO Users and USPTO Automated Information Systems. The users search the trademark information and documents using search criteria such as US Serial No., US Registration No., US Reference No. and, International Registration No. The users can view and download the status information and documents in multiple formats such as HTML, PDF, and JPEG.

Trademark Reporting and Data Mart (TRDM)
> TRDM provides business reports and dashboards connecting to respective data sources. It provides enhanced reporting capabilities that are more flexible and accessible to Trademark Management by allowing a user to create and query using a semantic layer interface between the user and the data source. Users can also view, print, and export reports to common file formats from the end-user workstation. Data visualization creation and viewing are also available.

Trademark Electronic Official Gazette (TMeOG)

> TMeOG enables consumers of published data in the official gazette to review information and search for items of interest. It also provides individual users with the ability to download only those cases of interest to them instead of a whole publication, allowing for both easier to use documents as well as an easier integration process with 3rd party applications.

Trademark Next Generation Identification Master List System (TMNG-IDM)

> TMNG-IDM provides an editable and searchable version of the USPTO's ID Manual as well as customizable user-interface versions for internal and external users including: system administrator and editors (core users); examining attorneys; trademark personnel; international partners; and trademark owners, applicants, registrants and their representatives.
>
> It allows authorized users to perform editing functions and provides role-based search capability across current and archival versions. It also provides improved search and retrieval capability by including filters for Nice Classification (NCL) year, which allows a more focused search, as terms for goods and services change over time. The system also provides additional detail by displaying color-coded results to distinguish fully matched from partially matched elements.

TMNG Internal

> TMNG Internal is used by Examining Attorneys during the Examination phase of an application. Over time, TMNG Internal will be extended to support additional phases of the trademark lifecycle, including Pre-Exam, Madrid Processing, and Statement of Use (SOU).

Trademark Next Generation e-File (eFile)

> eFile is still under development. Once completed, it will be used by customers to submit/make changes to Trademark Applications, replacing the legacy TEAS and TEASi applications.

Trademark Next Generation Content Management System (TMNG_CMS)

> TMNG_CMS provides a single modern content repository that is used by all TMNG internal systems.

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

Trademark examiners use the TMNG Internal system to access the applications that have been assigned to them. The examiner processes the application, using the Trademark Processing System – Internal Systems (TPS-IS) AIS X-Search to research potentially conflicting marks, and determines if the registration should be granted or denied. Registrations, whether processed by examiners using TMNG or TPS-IS, are published by the Trademark Electronic Official Gazette.

(c) any information sharing conducted by the system
TMNG shares trademark data with the Trademark Processing System – Internal Systems (TPS-IS). TPS-IS is the legacy system where trademark applicant data is stored. TMNG synchronizes this data, so that trademark examiners can 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 FIPS 199 security categorization for TMNG 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):					

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 is 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: TMNG connects with and receives data from the TRAM component of TPS-IS. The information transmitted between the systems is protected within USPTO's secure perimeter through the Network and Security Infrastructure (NSI) and the Enterprise Monitoring and Security Operations (EMSO) systems.
☐	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 does not have access to the entire system, only the public-facing components, through which they will have access to the publically releasable PII stored by the 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: The PII stored by TMNG is collected by the TPS-ES system. A notice is provided by a warning banner when the applicant accesses the TPS-ES system to submit the information. 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): _November 27, 2017_____ ☐ 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 TMNG. 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 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 TMNG. The overall FIPS 199 security impact level for TMNG 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 TMNG 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.

Windows and Linux servers within TMNG are regularly updated with the latest security patches by the Windows and Unix System Support Groups.

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 (date).
☐	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: AASSO: Non-record 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 N1-241-05-2:5: Information Dissemination Product Reference
☐	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 TMNG is public record information.
☒	Context of Use	Provide explanation: The personally identifiable information processed by TMNG 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.