Template Version Number: 01-2021

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

Privacy Threshold Analysis
for the
Trademark Next Generation

U.S. Department of Commerce Privacy Threshold Analysis

USPTO Trademark Next Generation

Unique Project Identifier: PTOT-004-00

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

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

The Trademark Next Generation (TMNG) is an application information system that provides support for the automated processing of trademark applications for the USPTO. TMNG provides users with bibliographic data in a standard markup form, business reporting and dashboard data sources. Publishing features are available to enable consumer's access to published data in the official gazette to review information and search for items of interest. Editing features allow authorized users to perform editing functions (create, modify, delete) that are role-based for searching across current and archival versions. TMNG is also used by Examining Attorneys during the Examination phase of an application.

Address the following elements:

a) *Whether it is a general support system, major application, or other type of system*
Trademark Next Generation (TMNG) is a major application.

b) *System location*

Trademark Next Generation (TMNG) is located at Alexandria, VA.

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

TMNG interconnects with the following systems below:

Corporate Web Systems (CWS): The CWS provides a feature-rich and stable platform that contains PTOWeb, Image Gallery and RDMS.

Database Services (DBS): DBS is an Infrastructure information system and provides a Database Infrastructure to support mission of USPTO database needs.

Enterprise Desktop Platform (EDP): The EDP is an infrastructure information system that provides a standard enterprise-wide environment that manages desktops and laptops running on the Windows operating system (OS), providing United States Government Configuration Baseline (USGCB) compliant workstations.

Enterprise Software Services (ESS): Enterprise Software Services provides the USPTO organization with a collection of programs that utilize common business applications and tools for modeling how the entire organization works. In addition, ESS provides a centralized solution for assisting developers in building applications unique to the organization. The software implemented is intended to solve an enterprise-wide problem, rather than specific departmental issues. Enterprise level software aims to improve the enterprise's productivity and efficiency by providing business logic and support functionality, continuous collaborative and communication tools for organizational personnel to complete their everyday task.

Enterprise UNIX Services (EUS): The EUS System consists of assorted UNIX operating system variants (OS) each comprised of many utilities along with the master control program - the kernel.

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

ICAM-Identity as a Service (ICAM-IDaaS): ICAM-IDaaS provides unified access management across applications and API based on single sign-on service. Identity and access management is provided by Okta's cloud-based solution which uses Universal Directory to create and manage users and groups.

Network and Security Infrastructure System (NSI): The 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 United States Patent and Trademark Office (USPTO) IT applications.

Open Data/Big Data Master (OD/BD): The Open Data/Big Data (OD/BD) master system consists of subsystems which support the Big Data Portfolio. OD/BD resides on the UACS platform, which employs IaaS and PaaS services from AWS. The current subsystems under this master system consists of Big Data Reservoir (BDR), Developer Hub (DH), Collection of Economic Analysis Tools (COEAT), Bulk Data Storage System (BDSS) and Developer Hub Assignment Search (DH-AS).

Security and Compliance Services (SCS): 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): SIMS is a Storage Infrastructure information service that 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. It is accessible to servers so that the devices appear like locally attached devices to the operating system. SIMS has its own network of storage devices that are generally not accessible through the local area network (LAN) by other devices.

Service Oriented Infrastructure (SOI): SOI provides stable platforms and feature-rich services upon which USPTO applications can deploy.

Trademark External (TE): TM External Search is comprised of different search components, which includes EFile, TSDR, TM-PEA, TM-eOG, and TM-NS.

Trademark Exam (TM-EXM): is a center where trademark attorneys and professional staff have the ability to securely login and complete end-to-end review and processing of trademark applications/registrations.

Trademark Processing System – External System (TPS ES): The purpose of this system is to provide service support for processing trademark applications for USPTO.

Trademark Processing System – Internal System (TPS IS): The purpose of this system is to provide service support for processing trademark applications for USPTO.

Trademark Trial and Appeal Board Center (TTABC): The TTAB Center is an application information system, and provides an online interface for USPTO customers to submit forms to the Trademark Trial and Appeal Board (TTAB) electronically.

USPTO AWS Cloud Services (UACS) EIPL-IHSC: The UACS General Support System (GSS) is a standard infrastructure platform used to support PTO Application Information Systems (AIS) hosted in the AWS East/West environment.

d) The purpose that the system is designed to serve

The TMNG is an application information system that provides support for the automated processing of trademark applications for the USPTO.

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

TMNG is an application information system, and provides support for the automated processing of trademark applications for the USPTO. It is comprised of the following six Automated Information Systems (AIS).

- Trademark Status and Document Retrieval (TSDR) provides bibliographic data in a standard markup form.
- Trademark Electronic Official Gazette (TMeOG) enable consumers of published data in the official gazette to review information and search for items of interest.
- Trademark Next Generation Identification Master List System (TMNG-IDM) allows authorized users to perform editing functions (create, modify, delete), provide role-based, searching across current and archival versions.
- TMNG Examination (formerly TMNG Internal System) is used by Examining Attorneys during the Examination phase of an application.
- Trademark Next Generation Content Management System (TMNG-CMS) purpose is to transition to a single modern content repository that will be used by all TMNG Examination systems.

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

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

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

Federal employees, contractors, members of the public.
Note: Only a part of the application is public facing and available to the general public. The general public will have access to only stored PII that is able to be released for public consumption.

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

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

i) How information is transmitted to and from the system

TMNG uses HTTPS (Hypertext Transfer Protocol Secure) for transmitting to and from the system over the USPTO internal network, as well as the public internet. All external connections with systems outside of the USPTO are employed through Network and Security Infrastructure System (NSI).

Questionnaire:

1. Status of the Information System
1a. What is the status of this information system?

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

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

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

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

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

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

☐ Yes. This is a new information system.

☐ Yes. This is an existing information system for which an amended contract is needed.

☐ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

☒ No. This is not a new information system.

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

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

☐ Yes. *(Check all that apply.)*

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

☒ No.

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

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

☐ Yes, the IT system collects, maintains, or disseminates BII.

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

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

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

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

☐ DOC employees

☐ Contractors working on behalf of DOC
☐ Other Federal Government personnel
☒ Members of the public

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

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

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

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

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

☒ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

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

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

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

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?
Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

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

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

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

CERTIFICATION

☒ The criteria implied by one or more of the questions above **apply** to the Trademark Next Generation and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

☐ The criteria implied by the questions above **do not apply** to the Trademark Next Generation and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

System Owner Name: Donald Ulrich Office: Trademark Systems Division (I/AEDTSD) Phone: (571) 272-1093 Email: Donald.Ulrich@uspto.gov Signature: Users, Ulrich, Donald Digitally signed by Users, Ulrich, Donald Date: 2023.07.28 07:51:59 -04'00' Date signed: ________________________________	**Chief Information Security Officer** Name: Timothy S. Goodwin Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-0653 Email: Timothy.Goodwin@uspto.gov Signature: Digitally signed by Timothy Goodwin Date: 2023.08.08 08:48:22 -04'00' Date signed: ________________________________
Privacy Act Officer Name: Kyu Lee Office: Office of General Law (O/GL) Phone: (571) 272-6421 Email: Kyu.Lee@uspto.gov Signature: Users, Lee, Kyu S. Digitally signed by Users, Lee, Kyu S. Date: 2023.08.04 18:55:08 -04'00' Date signed: ________________________________	**Bureau Chief Privacy Officer and Co-Authorizing Official** Name: Henry J. Holcombe Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-9400 Email: Jamie.Holcombe@uspto.gov Signature: Users, Stephens, Deborah Digitally signed by Users, Stephens, Deborah Date: 2023.08.08 10:55:10 -04'00' Date signed: ________________________________
Co-Authorizing Official Name: David Gooder Office: Office of the Trademarks Phone: (571) 270-0980 Email: David.Gooder@uspto.gov Signature: Users, Gooder, David S. Digitally signed by Users, Gooder, David S. Date: 2023.08.14 16:21:34 -04'00' Date signed: ________________________________	