Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
Trademark Next Generation

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

Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry
Date: 2023.08.09 09:26:06 -04'00'

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 brief description of the information system.

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

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.

(e) 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.

(f) 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).

(g) Any information sharing
TMNG shares trademark registration information with the public, via the Internet. Additionally, within USPTO, TMNG shares trademark data with the 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.

(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. § 1051 et seq.; 37 CFR § 2.21.

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

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.

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

Section 2: Information in the System

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

Identifying Numbers (IN)					
a. Social Security*	☐	f. Driver's License	☐	j. Financial Account	☐
b. Taxpayer ID	☐	g. Passport	☐	k. Financial Transaction	☐
c. Employer ID	☐	h. Alien Registration	☐	l. Vehicle Identifier	☐
d. Employee ID	☐	i. Credit Card	☐	m. Medical Record	☐
e. File/Case ID	☐				
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	☒	h. Date of Birth	☐	o. Financial Information	☐
b. Maiden Name	☐	i. Place of Birth	☐	p. Medical Information	☐
c. Alias	☐	j. Home Address	☒	q. Military Service	☐
d. Gender	☐	k. Telephone Number	☒	r. Criminal Record	☐
e. Age	☐	l. Email Address	☒	s. Marital Status	☐
f. Race/Ethnicity	☐	m. Education	☐	t. Mother's Maiden Name	☐
g. Citizenship	☐	n. Religion	☐		
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	☒	e. Work Email Address	☒	i. Business Associates	☒

b. Job Title	☐	f. Salary	☐	j. Proprietary or Business Information	☐
c. Work Address	☒	g. Work History	☐	k. Procurement/contracting records	☐
d. Work Telephone Number	☒	h. Employment Performance Ratings or other Performance Information	☐		
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	☐	f. Scars, Marks, Tattoos	☐	k. Signatures	☐
b. Palm Prints	☐	g. Hair Color	☐	l. Vascular Scans	☐
c. Voice/Audio Recording	☐	h. Eye Color	☐	m. DNA Sample or Profile	☐
d. Video Recording	☐	i. Height	☐	n. Retina/Iris Scans	☐
e. Photographs	☐	j. Weight	☐	o. Dental Profile	☐
p. 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	☒	f. 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 Describe how the accuracy of the information in the system is ensured.

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

2.4 Is the information covered by the Paperwork Reduction Act?

☒	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. 0651-0050: Response to Office Action & Voluntary Amendment Forms 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
☐	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	☐	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): Click or tap here to enter text.			

☒	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			
For a Computer Matching Program	☐	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's 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. As anyone may register a trademark, the information may reference a federal employee, contractor, member of the public or a foreign national- for the purposes of this PIA, we will consider the above all part of members of the public. Trademark registrant PII is shared with the public as part of information sharing initiatives.

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

The information is published to the public. There are no potential threats to privacy, as the information is not private. (See section 7.1)
All data transmissions not done through dedicated lines require security certificates. Inbound transmissions as well as outbound transmissions pass through a DMZ before being sent to endpoint servers. Access controls, auditing and encryption are leveraged to prevent PII/BII leakage.

In accordance with the USPTO Privacy Policy guidelines, all systems that process PII and have interconnections are designed and administered to ensure the integrity of PII provided to and by TMNG. Specific safeguards that are employed by the systems:

• The systems and its facility are physically secured and closely monitored. Only individuals authorized by USPTO are granted logical access to the system.
• Technical, operational, and management security controls are in place and are verified regularly.
• Periodic security testing is conducted on the systems to help detect new security vulnerabilities on time. All personnel are trained to securely handle PII information and to understand their responsibilities for protecting PII.

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

☐	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
☒	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
☐	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.

☒	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 SCS systems. - ESS - ICAM-IDaaS - TPS-ES - TPS-IS All data transmissions not done through dedicated lines require security certificates. Inbound transmissions as well as outbound transmissions pass through a DMZ before being sent to endpoint servers. Access controls, auditing and encryption are leveraged to prevent PII/BII leakage. In accordance with the USPTO Privacy Policy guidelines, all systems that process PII and have interconnections are designed and administered to ensure the integrity of PII provided to and by TMNG. Specific safeguards that are employed by the systems: • The systems and its facility are physically secured and closely monitored. Only individuals authorized by USPTO are granted logical access to the system. • Technical, operational, and management security controls are in place and are verified regularly. • Periodic security testing is conducted on the systems to help detect new security vulnerabilities on time. All personnel are trained to securely handle PII information and to understand their responsibilities for protecting PII.
☐	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	☒	Government Employees	☒
Contractors	☒		
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.)*

☒	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: https://www.uspto.gov/privacy-policy https://www.uspto.gov/trademarks/apply/teas-and-teasi-paperwork-reduction-act-burden#TEAS- Privacy-Act-Statement	
☒	Yes, notice is provided by other means.	Specify how: The PII stored by TMNG is collected by the TPSES 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.
☐	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:
☒	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: For USPTO to review, process and potentially issue a trademark to an individual the PII/BII requested must be provided. If the information is not provided, USPTO would not be able to process the request and provide the individual a trademark.

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:
☒	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: TMNG processes and publishes the minimum amount of PII legally required for Trademarks. An individual is required to provide this information and is unable to consent to a particular use of their PII. The individual is made aware that the information provided will be made public.

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:

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

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: Audit Logs
☒	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): 11/10/2022 ☐ 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 (POA&M).
☒	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
☒	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
☒	Contracts with customers establish DOC 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. *(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 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 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."

☒	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: COMMERCE/PAT-TM-26, Trademark Application and Registration Records
☐	Yes, a SORN has been submitted to the Department for approval on (date).
☐	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.)*

☒	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 N1-241-05-2:5: Information Dissemination Product Reference GRS 4.1:010, Tracking and Control Records N1-241-05-2:1a: U.S. Patent and Trademark Office Core Publications
☐	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 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.)*

☒	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 level. *(Check all that apply.)*

☒	Identifiability	Provide explanation: Name, Home address, Telephone number, email address, work address and work phone number are non-sensitive identifiers.
☒	Quantity of PII	Provide explanation: There are hundreds of thousands of applications containing PII processed using TMNG each year.
☒	Data Field Sensitivity	Provide explanation: The data includes limited personal and work-related elements.
☒	Context of Use	Provide explanation: The personally identifiable information processed by TMNG is used to identify the individuals or companies and governments that have registered trademarks with the government of the United States.
☒	Obligation to Protect Confidentiality	Provide explanation: TMNG is obligated to protect confidentiality of PII in accordance with the Privacy Act of 1974, Federal Information Security Management Act (FISMA), E-Government

		Act of 2002, Section 208 and other federal regulations.
☒	Access to and Location of PII	Provide explanation: Trademark Next Generation (TMNG) is located at 600 Dulany Street, Alexandria, VA 22314, on the 3rd floor, east wing at the Data Center. Access to the data center is only granted to individuals who are on an access list. Individuals requiring access to the data center must adhere to the data center's procedures.
☐	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 information is published to the public based on Okta access to the data and two-factor authentication. There are no potential threats to privacy, as the information is not private.

12.2 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.

12.3 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.