


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



**Privacy Impact Assessment
for the
Intellectual Property Leadership Management Support System
(IPLMSS)**

Reviewed by: Deborah Stephens, 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

 Digitally signed by BRIAN ANDERSON
Date: 2025.11.10 15:24:27 -05'00'

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

Date

U.S. Department of Commerce Privacy Impact Assessment USPTO Intellectual Property Leadership Management Support System (IPLMSS)

Unique Project Identifier: PTOL-001-00

Introduction: System Description

Provide a brief description of the information system.

Intellectual Property Leadership Management Support System (IPLMSS) is a Major Application which facilitates grouping and management of 5 separate Automated Information Systems (AISs) boundaries that collectively support the United States Patent and Trademark Office's (USPTO) Director, Deputy Director, Office of the General Counsel (OGC), including OGC's components the Office of General Law (OGL), Office of the Solicitor, and Office of Enrollment and Discipline (OED), Trademark Trial and Appeal Board (TTAB), and Office of Policy and International Affairs (OPIA). The following AISs make up IPLMSS:

- **Electronic System for Trademark Trials and Appeals (ESTTA):**
A web-based system for customers to electronically submit forms to the TTAB.
- **General Counsel Case Tracking System (GCCTS):**
A legal practice management system used by the Solicitor's Office to handle case docketing, document management, text searching, scheduling, and contact management.
- **Office of the Enrollment and Discipline Information System (OEDIS):**
A critical system that supports the USPTO in meeting statutory obligations related to the application, registration, maintenance, and discipline of patent practitioners. Additionally, OEDIS has a public facing component which allows members of the public to search for registered attorneys and agents from the official roster, enables applicants and patent practitioners to update their contact information, submit requests to the USPTO and pay fees online, and manage their applications and registrations.
- **Trademark Trial and Appeal Board VUE (TTABVUE):**
Provides online access to view and print publicly available TTAB case filings but excludes confidential content.
- **Trademark Trial and Appeal Board Information System (TTABIS):**
An internal system that supports the TTAB in managing proceedings, tracking case status, generating actions, and issuing reports.

Address the following elements:

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

IPLMSS is a Major Application.

(b) System location

Manassas, Virginia.

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

IPLMSS is a Major Application that interconnects with the following separately accredited USPTO AISs:

Google Analytics: In compliance with the federal Digital Strategy, USPTO participates in the General Services Administration (GSA's) Digital Analytics Program (DAP) to capture metrics on web traffic for each public-facing system. The DAP uses the Google Analytics service for this capture. USPTO has licensed its own account for Google Analytics to supplement the DAP with metrics capture for all internal-use systems as well. Website Management Branch (WMB) coordinates the implementation of Google Analytics for all systems with the Google Tag Manager tool. The metrics are not directly used in supporting or troubleshooting technical issues with any AIS, but they can be important to the system owners and stakeholders (e.g., line of business or sponsor) in evaluation of the system's business goals.

Prometric: USPTO Office of Enrollment and Discipline (OED) launched an online exam applicant portal where applicants can apply or reapply for the Registration Examination. Prior to the launch, OED only accepted applications sent through postal mail. The online portal allows applicants to fill out forms, upload supporting documentation, and pay applicable examination and application fees for immediate receipt by OED. Designed to be a practical and simple self-service portal, OED continually looks for ways to use technology to create a user-friendly experience for applicants to conduct transactions with the office.

MyUSPTO Cloud: A collection of communication and customer relationship-focused solutions that provides secure and accessible electronic 'front doors' to the USPTO enabling the public and staff to easily connect to Patent and Trademark content & tools, exchange information, and improve customer and employee experiences.

Identity, Credential, and Access Management - Identity as a Service (ICAM-IDaaS):

The mission of the ICAM-IDaaS is to provide an enterprise authentication and authorization service to all applications/AIS's.

Data Storage Management System (DSMS): centralized data storage for application programs and code, databases, files, media, email, and other forms of information.

Storage Infrastructure Managed Service (SIMS): is part of Infra/Hosting Services Storage Data Storage Management System (DSMS).

Madrid International Trademark System (MITS): assists the Office of Trademark in sending, receiving, reviewing and verifying data from International Bureau (IB)-related to international applications that are being handled by the USPTO as governed by the Madrid Protocol.

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 (TPS-ES): is major application information system, and provides customer support for processing trademark applications for USPTO.

Enterprise Software Services (ESS): is comprised of multiple on premise and in-the-cloud software services, which support the USPTO in carrying out its daily tasks.

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

Enrollment and Discipline Information Technology System (EDITS): is a repository of documents serving the OED and conforms to USPTO IT infrastructure, platform and application requirements specified by the Chief Information Officer (CIO). EDITS documents are stored, made searchable and retrievable through OEDIS.

Service Oriented Infrastructure System (SOI): is a General Support System (GSS) (Infrastructure information system) that provides the underlying services which provide a mobile, feature-rich, and stable platform upon which USPTO applications can be deployed.

Enterprise Desktop Platform (EDP): is an infrastructure information system which provides a standard enterprise-wide environment that manages desktops and laptops

providing United States Government Configuration Baseline (USGCB) compliant workstations.

Security and Compliance Services (SCS): is a general support system that provides an integrated enterprise log management, event management, network behavior analysis, and reporting through the collection of events and network/application flow etc.

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

Enterprise Unix Services (EUS): is an infrastructure operating system with a sole purpose of providing a UNIX base hosting platform to support other systems at USPTO.

Network and Security Infrastructure System (NSI): facilitates the communications, secure access, protective services, and network infrastructure support for all USPTO applications.

One Patent Services Gateway (OPSG) subsystem of Patent Capture and Application Processing System - Capture and Initial Processing (PCAPS-IP): is comprised of multiple AIS that perform specific functions, including submissions, categorization, metadata capture, and patent examiner assignment of patent applications.

One Patent Services Gateway (OPSG) subsystem of Patent Capture and Application Processing System - Examination Support (PCAPS-ES): purpose is to process, transmit and store data and images to support the data-capture and conversion requirements of the USPTO to support the USPTO patent application process.

Trademark Processing System - Internal Systems (TPS-IS): is designed to capture, store, retrieve, and print digital images of trademark application documents. Through USPTO's website, the public can query the Portable Document Format (PDF) document to determine active fastener insignias. It processes the PII data collected by Trademark Processing System - External Systems (TPS-ES) as part of the trademark application process.

Click2Mail: is leveraged for automating USPTO direct mailing for OEDIS. Click2mail is utilized to automate printing, folding and mailing USPTO direct communication to patent applicants and practitioners. USPTO utilizes the Representational State Transfer (REST) API.

Fee Processing Next Generation (FPNG): includes fee management for external customers (Financial Manager, payment page / services, and fee services consumed by other systems)

and fee management for internal customers (e.g. Fee Processing Portal for processing fees and refunds).

Trademark Trial and Appeal Board Center (TTAB): is an application information system, and provides an online interface for USPTO customers to submit forms to the Trademark Trial and Appeal Board electronically. Using a Web-based interface, TTAB public customers can complete and submit these trademark forms electronically over the Internet.

Trademark Next Generation (TMNG): is an application information system that provides support for the automated processing of trademark applications for the USPTO.

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

IPLMSS provides capabilities and functionalities to support attorneys, litigation support personnel, USPTO staff, and the public. Attorneys and litigation support personnel use the system to cull and organize large amounts of Electronically Stored Information (ESI) via a Commercial-off-the-shelf (COTS) software and manage cases, documents, contracts, generate reports, and manage administrative documents.

- ESTTA – provides an online interface for USPTO customers to submit forms to the TTAB electronically. Using a Web-based interface, ESTTA customers can complete and submit these trademark forms electronically over the internet. The TTAB application form is for public, who can also be customers, to complete online and submit to the USPTO. The electronic submissions are then transferred to the TTABIS for normal intake processing.
- GCCTS – is a legal practice management system used by the Solicitor’s Office for docketing cases and managing documents and contacts. The GCCTS is a COTS application which performs the following: case docketing, document management, document full text searching, ticklers, calendar scheduling, and contact management.
- OEDIS is an AIS that supports the OED at USPTO. It is comprised of two main subsystems: OEDIS Core and OEDIS CI.
OEDIS Core– is a secure intranet web application used internally by OED staff to manage the full lifecycle of patent practitioners. This includes receiving and processing applications for registration, maintaining the official practitioner roster, tracking disciplinary matters, and issuing notices—personalized or otherwise—through Click2Mail. Each year, OED processes thousands of documents through OEDIS,

including applications, registration materials, supporting documentation, roster updates, grievances, among other documents.

OEDIS CI– is the public-facing component of the system. It allows the public to search the official roster of registered patent attorneys and agents online. Practitioners can use the portal to update their contact information, submit requests to OED, and pay fees electronically. Applicants may apply or reapply for the Examination for Registration, upload supporting documentation, and pay related application and examination fees through the same interface.

- **TTABVUE** – allows USPTO employees and contractors and public users to view Trademark Trial and Appeals Board proceedings with scanned incoming filings from the Internet. It also allows the user to print, enlarge the incoming document to a readable size. It does not, however, allow the user to see the notes, attachments, and any confidential information in the document.
- **TTABIS** – provides integrated information support to the TTAB of the USPTO in processing all Proceedings brought before the Board. TTABIS enables TTAB staff to view filings, generate actions, track the status of proceedings, record data, and produce reports to support management information about TTAB.

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

ESTTA

The user submits filing with TTAB through the public facing website application. The application does not have specified accounts within the system therefore no approved access or training is required.

GCCTS

The privilege user retrieves information through the internal only website application and users must have an existing USPTO PTONet (Active Directory) account prior with GCCTS privileged granted access. After user authenticates through Single Sign-On (SSO) access to with group and role membership by the account manager.

OEDIS

OEDIS-CI and OEDIS-Core uses Okta OpenID Connect (OIDC) user identity. The application provides user IDs and passwords generated by application for specific user roles. Access roles to the application must be assigned manually by the OEDIS Administrator team to ensure the most restrictive operation.

TTAB-VUE

The user retrieves information through website application and does not have specified accounts within the system.

TTABIS

The internal user process information through Single Sign On (SSO) and application roles.

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

ESTTA

The public application for trademark document utilizes web application Transmission Control Protocol (TCP) port Hypertext Transfer Protocol Secure (HTTPS) communications, to ensure secure data transmission over the internet by encrypting data between the client and server, protecting it from eavesdropping and tampering.

GCCTS

The internal only website application utilizes web application TCP port HTTPS communications, to ensure secure data transmission over the internet by encrypting data between the client and server, protecting it from eavesdropping and tampering.

OEDIS

OEDIS utilizes web application TCP port HTTPS communications, to ensure secure data transmission over the internet by encrypting data between the client and server, protecting it from eavesdropping and tampering. In addition, business unit users (internal) utilize commercial Secure File Transfer Protocol (SFTP) for transferring files to Prometric. Furthermore, paper application is available for the public to be mail/fax for manual data entry by OED staff.

TTABIS

The internal application utilizes desktop application, to ensure secure data transmission over the internet by encrypting data between the client and server, protecting it from eavesdropping and tampering.

TTAB-VUE

The website application utilizes web application TCP port HTTPS communications, to ensure secure data transmission over the internet by encrypting data between the client and server, protecting it from eavesdropping and tampering.

(g) Any information sharing

Yes, there are specific instances whereby information is required by law to be shared to the public (i.e., FOIA/Privacy Act or e-Discovery requests) or in support of litigation(s).

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

35 USC § 2(b)(2) [Patent Practitioners], 35 USC § 6 [PTAB proceedings], 37 CFR § 11

Subpart C– [Investigations and Disciplinary Proceedings; Jurisdiction, Sanctions, Investigations, and Proceedings], 37 CFR § 11.7 [Registration Applicants], 37 CFR § 11.9(b) [Limited Recognition Applicants], 35 USC §§ 1.6 and 31 [Registration Applicants], 15 USC § 1051 et seq. [TTAB proceedings], 5 USC § 552a [Privacy Act requests], 5 USC § 552 [Freedom of Information Act requests], Federal Rule of Civil Procedure 34 [Discovery in Civil Litigation]

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

Moderate

Section 1: Status of the Information System

- 1.1 Indicate whether the information system is a new or existing system.

- ☐ This is a new information system.
- ☐ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

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

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

Section 2: Information in the System

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

Identifying Numbers (IN)					
a. Social Security*	<input checked="" type="checkbox"/>	f. Driver's License	<input checked="" type="checkbox"/>	j. Financial Account	<input checked="" type="checkbox"/>
b. Taxpayer ID	<input checked="" type="checkbox"/>	g. Passport	<input checked="" type="checkbox"/>	k. Financial Transaction	<input checked="" type="checkbox"/>
c. Employer ID	<input checked="" type="checkbox"/>	h. Alien Registration	<input checked="" type="checkbox"/>	l. Vehicle Identifier	<input checked="" type="checkbox"/>
d. Employee ID	<input checked="" type="checkbox"/>	i. Credit Card	<input checked="" type="checkbox"/>	m. Medical Record	<input checked="" type="checkbox"/>
e. File/Case ID	<input checked="" type="checkbox"/>				
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					
OEDIS: the SSN may be incidentally collected because of documents submitted to OED.					

General Personal Data (GPD)					
a. Name	<input checked="" type="checkbox"/>	h. Date of Birth	<input checked="" type="checkbox"/>	o. Financial Information	<input checked="" type="checkbox"/>
b. Maiden Name	<input checked="" type="checkbox"/>	i. Place of Birth	<input checked="" type="checkbox"/>	p. Medical Information	<input checked="" type="checkbox"/>
c. Alias	<input checked="" type="checkbox"/>	j. Home Address	<input checked="" type="checkbox"/>	q. Military Service	<input checked="" type="checkbox"/>
d. Sex	<input checked="" type="checkbox"/>	k. Telephone Number	<input checked="" type="checkbox"/>	r. Criminal Record	<input checked="" type="checkbox"/>
e. Age	<input checked="" type="checkbox"/>	l. Email Address	<input checked="" type="checkbox"/>	s. Marital Status	<input checked="" type="checkbox"/>
f. Race/Ethnicity	<input checked="" type="checkbox"/>	m. Education	<input checked="" type="checkbox"/>	t. Mother's Maiden Name	<input checked="" type="checkbox"/>
g. Citizenship	<input checked="" type="checkbox"/>	n. Religion	<input type="checkbox"/>		
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	<input checked="" type="checkbox"/>	e. Work Email Address	<input checked="" type="checkbox"/>	i. Business Associates	<input checked="" type="checkbox"/>
b. Job Title	<input checked="" type="checkbox"/>	f. Salary	<input checked="" type="checkbox"/>	j. Proprietary or Business Information	<input checked="" type="checkbox"/>
c. Work Address	<input checked="" type="checkbox"/>	g. Work History	<input checked="" type="checkbox"/>	k. Procurement/contracting records	<input checked="" type="checkbox"/>
d. Work Telephone Number	<input checked="" type="checkbox"/>	h. Employment Performance Ratings or other Performance Information	<input checked="" type="checkbox"/>		
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	<input type="checkbox"/>	f. Scars, Marks, Tattoos	<input type="checkbox"/>	k. Signatures	<input checked="" type="checkbox"/>

b. Palm Prints	<input type="checkbox"/>	g. Hair Color	<input checked="" type="checkbox"/>	l. Vascular Scans	<input type="checkbox"/>
c. Voice/Audio Recording	<input checked="" type="checkbox"/>	h. Eye Color	<input checked="" type="checkbox"/>	m. DNA Sample or Profile	<input type="checkbox"/>
d. Video Recording	<input checked="" type="checkbox"/>	i. Height	<input checked="" type="checkbox"/>	n. Retina/Iris Scans	<input type="checkbox"/>
e. Photographs	<input checked="" type="checkbox"/>	j. Weight	<input checked="" type="checkbox"/>	o. Dental Profile	<input type="checkbox"/>
p. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	<input checked="" type="checkbox"/>	c. Date/Time of Access	<input checked="" type="checkbox"/>	e. ID Files Accessed	<input type="checkbox"/>
b. IP Address	<input checked="" type="checkbox"/>	f. Queries Run	<input checked="" type="checkbox"/>	f. Contents of Files	<input type="checkbox"/>
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	<input checked="" type="checkbox"/>	Hard Copy: Mail/Fax	<input checked="" type="checkbox"/>	Online	<input checked="" type="checkbox"/>
Telephone	<input type="checkbox"/>	Email	<input checked="" type="checkbox"/>		
Other (specify):					

Government Sources					
Within the Bureau	<input checked="" type="checkbox"/>	Other DOC Bureaus	<input checked="" type="checkbox"/>	Other Federal Agencies	<input checked="" type="checkbox"/>
State, Local, Tribal	<input checked="" type="checkbox"/>	Foreign	<input checked="" type="checkbox"/>		
Other (specify):					

Non-government Sources					
Public Organizations	<input checked="" type="checkbox"/>	Private Sector	<input type="checkbox"/>	Commercial Data Brokers	<input type="checkbox"/>
Third Party Website or Application			<input type="checkbox"/>		
Other (specify):					

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

From an administrative implementation, the Office of the General Counsel's components have administrative and support staff that function as points of contacts whereby customers may directly contact for the administration of information accuracy. From a technical implementation, 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 expected by authorized users. Management controls are utilized to prevent the inappropriate disclosure of sensitive information. In addition, the Perimeter Network (NSI) and SCS provide additional automated transmission and monitoring mechanisms to ensure that PII/BII information is protected and not breached by external entities.

2.4 Is the information covered by the Paperwork Reduction Act?

<input checked="" type="checkbox"/>	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. 0651-0012 Admittance to Practice 0651-0017 Practitioner Conduct and Discipline 0651-0040 TTAB Actions 0651-0081 Law School Clinic Program
<input type="checkbox"/>	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNDP)			
Smart Cards	<input type="checkbox"/>	Biometrics	<input type="checkbox"/>
Caller-ID	<input type="checkbox"/>	Personal Identity Verification (PIV) Cards	<input type="checkbox"/>
Other (specify):			

<input checked="" type="checkbox"/>	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.
-------------------------------------	--

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings	<input type="checkbox"/>	Building entry readers	<input type="checkbox"/>
Video surveillance	<input type="checkbox"/>	Electronic purchase transactions	<input type="checkbox"/>
Other (specify): Click or tap here to enter text.			

<input checked="" type="checkbox"/>	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	<input type="checkbox"/>	For administering human resources programs	<input type="checkbox"/>
For administrative matters	<input checked="" type="checkbox"/>	To promote information sharing initiatives	<input checked="" type="checkbox"/>
For litigation	<input checked="" type="checkbox"/>	For criminal law enforcement activities	<input type="checkbox"/>
For civil enforcement activities	<input type="checkbox"/>	For intelligence activities	<input type="checkbox"/>
To improve Federal services online	<input checked="" type="checkbox"/>	For employee or customer satisfaction	<input type="checkbox"/>
For web measurement and customization technologies (single-session)	<input type="checkbox"/>	For web measurement and customization technologies (multi-session)	<input type="checkbox"/>
Other (specify):			

Section 5: Use of the Information

- 5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

[OEDIS] The PII (i.e., name, phone number, mailing/email address, birthdate, place of birth, education, reasonable accommodation information, and citizenship information) submitted by applicants or practitioners collected and maintained is used to determine eligibility to practice before the USPTO. The sensitive PII may reference federal employees.

[GCCTS] The stored PII may include portions or all references in Section 2.1 for IN, GPD, and WRD. The data is for internal Solicitors Office staff use only that supports legal case and document management and may contain confidential prosecution information that is not releasable to the public. The information may reference federal employees, members of the public, discipline of practitioners, and foreign nationals.

[ESTTA] The PII (i.e., name, telephone number, mailing and/or email address) is to the public to help improve federal services online.

[TTABVUE] There is no PII/BII available for public viewing. However, PII (i.e., name, telephone number, mailing and/or email address) is disseminated (viewable) to the public to help improve federal services online. The information may reference federal employees, members of the public and foreign nationals.

- 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.)

Inadvertent private information exposure to foreign entities or adversarial entities as well as insider threats are risks and USPTO has policies, procedures and training to ensure that employees are aware of their responsibility of protecting information and the negative impact to the agency if there is a loss, misuse, or unauthorized access to or modification of private information. USPTO requires annual security role-based training and annual mandatory security awareness procedure training for all employees. The following are USPTO current policies; Information Security Foreign Travel Policy (OCIO-POL-6), IT Privacy Policy – (OCIO-POL-18), IT Security Education Awareness Training Policy (OCIO-POL-19), Personally Identifiable Data Removal Policy (OCIOPOL-23), USPTO Rules of the Road (OCIO-POL-36). All offices of USPTO adhere to USPTO Records Management Office’s Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citation.

NIST security controls are in place to ensure that information is handled, retained, and disposed of appropriately. For example, advanced encryption is used to secure the data both during transmission and while stored at rest. Access to individual’s PII is controlled through the application and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. USPTO requires annual security role based training and annual mandatory security awareness procedure training for all employees. All offices adhere to the USPTO Records Management Office’s Comprehensive Records Schedule or the General Records Schedule and the corresponding disposition authorities or citations.

Section 6: Information Sharing and Access

- 6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DOC bureaus	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Federal agencies	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
State, local, tribal gov’t agencies	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Private sector	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign governments	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign entities	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other (specify): Court System	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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

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

<input type="checkbox"/>	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
<input checked="" type="checkbox"/>	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
<input type="checkbox"/>	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

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

<input checked="" type="checkbox"/>	<p>Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:</p> <p>ESS EDITS SCS PCAPS-ES TPS-IS PCAPS-IP Click2Mail Google Analytics MyUSPTO-C ICAM-IDaaS DSMS SIMS TM-EXM TPS-ES DBS FPNG TTAB TMNG</p> <p>Information is protected through a layered security approach which incorporates the use of secure authentication, access control, mandatory configuration settings, firewalls, Virtual Private Network (VPN), and encryption, where required. Internally within USPTO, data transmission confidentiality controls are provided by PTONet.</p> <p>All data transmissions are encrypted and require credential verification. 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.</p> <p>In accordance with the USPTO Privacy Policy guidelines, all systems that process PII and have interconnections are designed and administered to ensure the confidentiality of PII provided to and by IDSS.</p> <p>Specific safeguards that are employed by the systems:</p> <ul style="list-style-type: none"> • 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.
-------------------------------------	---

	<ul style="list-style-type: none"> • 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. <p>NIST security controls are in place to ensure that information is handled, retained, and disposed of appropriately. For example, advanced encryption is used to secure the data both during transmission and while stored at rest. Access to individual's PII is controlled through the application and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. USPTO requires annual security role based training and annual mandatory security awareness procedure training for all employees. All offices adhere to the USPTO Records Management Office's Comprehensive Records Schedule or the General Records Schedule and the corresponding disposition authorities or citations</p>
<input type="checkbox"/>	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public	<input checked="" type="checkbox"/>	Government Employees	<input checked="" type="checkbox"/>
Contractors	<input checked="" type="checkbox"/>		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

<input checked="" type="checkbox"/>	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.
<input checked="" type="checkbox"/>	<p>Yes, notice is provided by a privacy policy and Privacy Act Statement. The privacy policy can be found at: https://www.uspto.gov/privacy-policy</p> <p>OEDIS Privacy Act Statement: https://www.uspto.gov/sites/default/files/documents/PTO158_Application_for_Registration.pdf</p> <p>ESTTA: Applicants applying for Trademark Appeals are presented with a privacy policy statement as follows: https://estta.uspto.gov/</p> <p>TTABIS: NA</p> <p>TTABVUE: NA</p>

<input type="checkbox"/>	Yes, notice is provided by other means.	Specify how:
<input type="checkbox"/>	No, notice is not provided.	Specify why not:

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

<input type="checkbox"/>	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to decline to provide PII/BII.	<p>Specify why not:</p> <p>OEDIS: Patent attorneys/agents who wish to practice before the USPTO must provide the required information for their applications and registrations to be processed. At which time they may opt to decline to provide such information.</p> <p>ESTTA The appealing Trademark applicant grants consent by filing a trademark registration and submitting it for processing. They are notified that the information that they submit will become public information.</p> <p>TTABIS: It is a desktop application for internal users only.</p> <p>TTABVUE: It is a public search application for view only.</p>

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

<input type="checkbox"/>	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	<p>Specify why not:</p> <p>OEDIS: On the PTO158 form a registering Attorney/Agent applicant is notified of consent to use of their PII.</p> <p>ESTTA: Trademark applicants are provided the privacy policy statement during registration and are made aware of consent to the use of their PII.</p> <p>TTABIS: It is a desktop application for internal users only.</p> <p>TTABVUE: It is a public search application for view only.</p>

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

<input checked="" type="checkbox"/>	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	<p>Specify how:</p> <p>TTABIS: Only TTAB Admin role can update PII/BII.</p>
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	<p>Specify why not:</p> <p>OEDIS: During the online registration process, the Attorney/Agent are allocated the opportunity to ensure</p>

	<p>information accuracy. After registration Attorney/Agent is also provided USPTO administrative points of contact to coordinate registrant information updates.</p> <p>ESTTA: During the online registration process the appealing Trademark applicants are allocated the opportunity to ensure information accuracy. After registering a Trademark board appeal, applicants are also provided USPTO points of contact to coordinate applicant information updates.</p> <p>TTABVUE: It is a public search application for view only.</p>
--	---

Section 8: Administrative and Technological Controls

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

<input type="checkbox"/>	All users signed a confidentiality agreement or non-disclosure agreement.
<input type="checkbox"/>	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
<input checked="" type="checkbox"/>	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
<input checked="" type="checkbox"/>	Access to the PII/BII is restricted to authorized personnel only.
<input checked="" type="checkbox"/>	<p>Access to the PII/BII is being monitored, tracked, or recorded.</p> <p>Explanation: Technical control-USPTO employees (government/contractors) are required to have Active Directory (AD) user accounts for authentication and authorization to access USPTO resources. AD accounts are restrictive by default and are permissioned access to PII/BII after administrative vetting to confirm the employee requires access based on a need-to-know.</p>
<input checked="" type="checkbox"/>	<p>The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements.</p> <p>Provide date of most recent Assessment and Authorization (A&A): 8/13/2025</p> <p><input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.</p>
<input checked="" type="checkbox"/>	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
<input checked="" type="checkbox"/>	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 5 recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
<input checked="" type="checkbox"/>	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
<input checked="" type="checkbox"/>	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
<input type="checkbox"/>	Contracts with customers establish DOC ownership rights over data including PII/BII.
<input type="checkbox"/>	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
<input checked="" type="checkbox"/>	Other (specify): USPTO employees and contractors are subjected to a code of conduct during employment onboarding.

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).*

PII in IPLMSS is secured using appropriate administrative, physical, and technical safeguards in accordance with the applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

All access has role-based restrictions, and individuals with access privileges have undergone vetting and suitability screening. Data is maintained in areas accessible only to authorized personnel. The USPTO maintains an audit trail and performs random periodic reviews to identify unauthorized access.

Additionally, IPLMSS is secured by various USPTO infrastructure components, including the NSI system and other OCIO established technical controls that includes end-to-end transport layer protocols and where applicable data-at-rest encryption.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g. name or Social Security number)?

☒ Yes, the PII/BII is searchable by a personal identifier.

☐ No, the PII/BII is not searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

<input checked="" type="checkbox"/>	<p>Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. <i>(list all that apply):</i></p> <p>COMMERCE/PAT-TM 1: Attorneys and Agents Registered to Practice Before the Office. COMMERCE/PAT-TM 2: Complaints, Investigations and Disciplinary Proceedings Relating to Registered Patent Attorneys and Agents. COMMERCE/PAT-TM 5: Non-Registered Persons Rendering Assistance to Patent Applicants. COMMERCE/DEPT-5: Freedom of Information Act and Privacy Act Request Records COMMERCE/DEPT-14, Litigation, Claims, and Administrative Proceeding Records USPTO-26 Trademark Application and Registration Records</p>
<input checked="" type="checkbox"/>	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
<input type="checkbox"/>	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

General Records Schedules (GRS) / National Archives

<input checked="" type="checkbox"/>	<p>There is an approved record control schedule. Provide the name of the record control schedule:</p> <p>OEDIS: Short-Term IP Legal Activity Office Operation Records: N1-241-09-1, b5.2 b-5-2 Enrollment Examination: N1-241-09-1: b4.1</p> <p>Enrollment and Discipline Application and Roster Maintenance Files: N1-241-09-1: b4.2</p> <p>Subject Files Related to Enrollment and Discipline: N1-241-09-1: b4.3</p> <p>Enrollment Examination Answer Sheets - Unsuccessful Applicants: N1-241-09-1: b4.4</p> <p>Administrative Law Files, Office of Enrollment and Discipline Appeal Case Files: N1-241-09-1: b4.5</p> <p>Enrollment Examination Answer Sheets - Successful Applicants: N1-241-09-1: b4.6</p> <p>Enrollment and Discipline Roster of Attorney's and Agents Registered to Practice Before the USPTO: N1-241-09-1: b4.7</p> <p>Director's OED Decision Files: N1-241-09-1: b4.8</p> <p>FOIA, Privacy Act, and classified documents administrative records: GRS 4.2:001</p> <p>Access and disclosure request files: GRS 4.2:020 GRS 3.1: General Technology Management Records</p> <p>Item - 020 Information technology operations and maintenance records. Which include access and audit logs.</p> <p>GRS 3.2. Information Systems Security Records, Item 010, 020, 040, 050 Which include system security logs.</p> <p><u>TTAB Record Schedules</u></p> <p>N1-241-09-1, b3.1 b-3-1 Trademark Trial and Appeal Proceedings and Related Indexes Case files of Board hearings and decisions on adversary proceedings Permanent: Transfer 5 years after close of case.</p> <p>N1-241-09-1, b3.2 b-3-2 Trademark Trial and Appeal Administrative Files Temporary: Delete/return when case is terminated or when no longer needed whichever is first.</p> <p>GRS 3.1: General Technology Management Records Item - 020 Information technology operations and maintenance records. Which include access and audit logs.</p> <p>GRS 3.2. Information Systems Security Records, Item 010, 020, 040, 050 Which include system security logs.</p>
<input type="checkbox"/>	<p>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:</p>

<input checked="" type="checkbox"/>	Yes, retention is monitored for compliance to the schedule.
<input type="checkbox"/>	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	<input checked="" type="checkbox"/>	Overwriting	<input type="checkbox"/>
Degaussing	<input type="checkbox"/>	Deleting	<input checked="" type="checkbox"/>
Other (specify):			

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

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

<input type="checkbox"/>	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
<input checked="" type="checkbox"/>	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
<input type="checkbox"/>	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact level. *(Check all that apply.)*

<input checked="" type="checkbox"/>	Identifiability	Provide explanation: Data fields captured in the PIA include PII, such as name; date of birth; SSN; home or work address and telephone number; work email address etc. These can all be used as personal identifiers.
<input checked="" type="checkbox"/>	Quantity of PII	Provide explanation: The quantity of PII in this system 100,000s, enough to warrant adequate protection.
<input checked="" type="checkbox"/>	Data Field Sensitivity	Provide explanation: The combination of name, proprietary business information, etc. can make the data fields more sensitive.
<input checked="" type="checkbox"/>	Context of Use	Provide explanation: The PII collected is for allowing attorneys and agents with licenses to practice before the US Patent and Trademark Office or request of Trademark Board appeal. Also, information may be used to support FOIA, E-discovery, or

		Privacy Act requests.
<input checked="" type="checkbox"/>	Obligation to Protect Confidentiality	Provide explanation: USPTO Privacy Policy requires the PII information collected within the system to be protected accordance with the Privacy Act of 1974, PII must be protected.
<input checked="" type="checkbox"/>	Access to and Location of PII	Provide explanation: Because some the information containing PII must be transmitted outside of the PTO environment, there is an added need to ensure the confidentiality of the information during transmission.
<input type="checkbox"/>	Other:	Provide explanation:

Section 12: Analysis

- 12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

USPTO have identified and evaluated potential threats to PII such as insider threats and adversarial entities which may cause a loss of confidentiality and integrity of information. Based upon USPTO's threat assessment the Agency has implemented baseline of security controls to mitigate these risks to sensitive information to an acceptable level. USPTO has policies, procedures and training to ensure that employees are aware of their responsibility of protecting sensitive information and the negative impact on the agency if there is a loss, misuse, or unauthorized access to or modification of sensitive private information. USPTO requires annual security role-based training and annual mandatory security awareness procedure training for all employees.

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

<input type="checkbox"/>	Yes, the conduct of this PIA results in required business process changes. Explanation:
<input checked="" type="checkbox"/>	No, the conduct of this PIA does not result in any required business process changes.

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

<input type="checkbox"/>	Yes, the conduct of this PIA results in required technology changes.
--------------------------	--

	Explanation:
<input checked="" type="checkbox"/>	No, the conduct of this PIA does not result in any required technology changes.

APPENDIX A

PRIVACY POLICY STATEMENT

The information collected on these forms allows the TTAB to determine whether a party is entitled to registration of a mark. Responses to the requests for information are required to obtain the requested action. All information collected will be made public. Gathering and providing the information will require an estimated 10 to 45 minutes, depending on the form you choose. Please direct comments on the time needed to complete this form, and/or suggestions for reducing this burden to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, Washington, DC 20231. Please note that the TTAB may not conduct or sponsor a collection of information using a form that does not display a valid OMB control number.