Template Version Number: 01-2021

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: 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: 2022.10.04 14:40:48 -04'00'

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.

IPLMSS is a Major Application which facilitates grouping and management of 9 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), Patent Trial and Appeal Board (P-TACTS); Office of Patent Training (OPT); and Office of Policy and International Affairs (OPIA). The following AISs make up IPLMSS:

1. E-Discovery Software System (EDSS) – EDSS is a full-featured E-Discovery Commercial Off-The-Shelf (COTS) product used within the Office of the General Counsel (OGC). Attorneys and litigation support personnel employ the tool in a variety of legal cases to help cull and organize the larger amounts of Electronically Stored Information (ESI) that are common today. EDSS may incidentally collect, store, and disseminate PII and BII, including SSN, as part of attorney searching for information for litigation or other legal.

2. Electronic System for Trademark Trials and Appeals (ESTTA) – ESTTA provides an online interface for USPTO customers to submit forms to the Trademark Trial and Appeal Board (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 general public, who can also be customers, to complete online and submit to the USPTO. The electronic submissions are then transferred to the Trademark Trial and Appeal Board Information System (TTABIS) for normal intake processing.

3. General Counsel Case Tracking System (GCCTS) – 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.

4. General Counsel Library System (GCLS) – GCLS is a COTS library management system used to manage library content for the Solicitor's Office and the Office of Policy and International Affairs (OPIA). Its functions include creating, updating, and deleting

catalog records, creating borrower records, and tracking books in the collection for ordering. GCLS manages the library catalogs and allows the librarians to create, edit, and delete catalog records, create borrower records, check out and check in library materials, track and query loan information, and keep track of the books for ordering (Serials Management). Users are able to search the catalogs using the Online Library Access Catalog interface.

5. Notice of Suit Processing System (NOSPS) – NOSPS is a custom developed application that allows the Solicitor's Office to route electronic Notice of Suit documents to the respective Patent and Trademark electronic application files. The Notice of Suit documents are sent to the agency from U.S. District Courts where there is a proceeding involving a Patent or Trademark. When these notices are received, the NOSPS provides a Graphic User Interface (GUI) for data entry personnel to key in the Patent and Trademark numbers on the Notices. A copy of the Notice document is then routed in the respective electronic application files.

6. Office of Enrollment and Discipline Item Bank (OEDIB) – OEDIB is used by the Office of Enrollment and Discipline to develop and maintain assessments. The OEDIB web application provides the item maintenance, examination delivery, and reporting needs for the OED staff.

7. Office of the Enrollment and Discipline Information System (OEDIS) – OEDIS is an AIS that supports the Office of Enrollment and Discipline (OED) of the United States Patent and Trademark Office. It consists of two subsystems: OEDIS Core and OEDIS CI (Customer Interface). OEDIS Core is an Intranet Web application that is used by the OED to process patent practitioner registration, maintain the practitioner roster, and monitor practitioner disciplinary actions. OED receives an average of 72,000 pieces of paper per year, which include applications for registration, supporting documents that are part of the admission evaluation, and change of address forms.

   OEDIS Core is used to input incoming correspondence and permit immediate online access for routing and reviewing. It allows OED to electronically track the status of applicants and practitioners.

   OEDIS CI allows the public to browse and search the official roster of registered patent attorneys and agents on the Internet; enables patent attorneys and agents to update their contact information, submit requests to IED, and pay fees online. Applicants may apply or reapply for admission to the Examination of Registration and pay application and examination fees online.

8. Trademark Trial and Appeal Board VUE (TTABVUE) – TTABVUE allows PTO and public users to view Trademark Trial and Appeals Board (TTAB) 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.

9. Trademark Trial and Appeal Board Information System (TTABIS) – TTABIS provides integrated information support to the Trademark Trial and Appeal Board (TTAB) of the USPTO in processing all Proceedings brought before the Board. The TTABIS enables the Board to generate actions, track the status of Proceedings, record data, and issue reports. The TTABIS also provide an interface with the Trademark Reporting and Monitoring System (TRAM), which tracks the physical location and status of trademark applications as they are processed within the organization, enabling TTABIS to support the customer service center in tracking and analyzing information and case requests from the public.

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
The IPLMSS resides at the USPTO facilities located in Alexandria, 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:

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.

CIDM (AASS) Agency Administrative Support System - (AASS) consists of several applications that provide consolidation of document imaging services, enables management and tracking of hardware/software assets, and enables Under Secretary of Commerce for Intellectual Property and USPTO Director to receive and respond to a wide range of official correspondences.

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) 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.

PALM (PCAPS-IP) PCAPS-IP Patent Capture and Application Processing System - Capture and Initial Processing (PCAPS-IP) is comprised of multiple Automated Information Systems (AIS) that perform specific functions, including submissions, categorization, metadata capture, and patent examiner assignment of patent applications.

PALM EXPO (PCAPS-ES) Patent Capture and Application Processing System - Examination Support (PCAPS-ES) the purpose of this system 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.

TRAM (TPS-IS) Trademark Processing System - Internal Systems (TPS-IS) TRAM provides support to all facets of trademark operations. TRAM includes a database consisting of bibliographic text and prosecution history data. TRAM also supports trademark operations from receipt of new applications to the publication of the TMOG and post-registration activities. The publicly-releasable PII collected by components of the Trademark Processing System-External Systems (TPS-ES) system is stored within TRAM.

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

(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 general 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, and library content. Litigation support personnel and USPTO staff use the system to route electronic Notice of Suit (NOS) documents via a GUI interface for data entry, create assessments via a web interface, generate reports, and manage administrative documents. USPTO personnel and staff have authorized restricted access. The general public retrieve public releasable information via an online interface and submit trademark and registration forms electronically over the Internet or mail/fax for intake and processing.

(e) How information in the system is retrieved by the user
The general public may retrieve publicly available information by the OEDIS (customer interface), Mail/Fax or email. USPTO personnel and staff have authorized-restricted access.

(f) How information is transmitted to and from the system
Information may be transmitted to/from IPLMSS online web portals, email, and mail/fax.

(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],
37 CFR § 11.7 [Registration Applicants],
37 CFR § 11.9(b) [Limited Recognition Applicants],
35 USC §§ 1.6 and 31 [Registration Applicants],
35 USC § 6 [PTAB proceedings],
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	☐	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): EDSS: the SSN may be incidentally collected as a result from either e-Discovery, FOIA or Privacy Act search requests of agency records.					
*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.

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?

☒	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 0651-0063 PTAB Actions 0651-0069 Patent Review and Derivation Proceedings 0651-0081 Law School Clinic Program
☐	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).

[EDSS] The temporarily collected PII/BII are incidental content that may include portions or all references in Section 2.1 for IN, GPD, and WRD from agency records. The PII/BII are only collected during official e-Discovery requests and prudently disseminated to authorized parties supporting the requests. EDSS limits the collection of PII/BII to a minimum as necessary to meet USPTO business purposes, mission and legal obligations. PII/BII redaction automation is not implemented due to the risk of jeopardizing legal proceedings due to the potential risk of data integrity compromise. However; manual redaction is implemented when content is released to authorized parties. EDSS eDiscovery collections are routinely reviewed for relevance and content is removed based upon adjudicated cases. The PII/BII may reference federal employees.

[OEDIS] The PII (i.e., name, phone number, mailing/email address, birthdate, citizenship, place of birth, education, reasonable accommodation information, and alien registration information) submitted by applicants is collected and maintained and is used to determine eligibility to practice before the USPTO, regulate discipline, and communicate as required. 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.

[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.

[GCLS] The stored PII may include GPD and WRD data used for administrative and litigation purposes such as creating and updating catalog records or creating and maintaining borrower records in the library management system about attorneys.

[NOSPS] – The PII data collected may include GPD and WRD such as proprietary business information as it relates to NOS documents sent in litigation proceedings. The information may reference federal employees, members of the public, practitioners, and foreign nationals.

[OEDIB] –The collected PII data may include GPD and WRD for the purpose of administering and processing patent practitioner registration, maintaining the practitioner roster, and monitoring practitioner disciplinary actions.

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 of the USPTO adhere to the USPTO Records Management Office's Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citation.

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: ESS AASS SCS PCAPS-ES TPS-IS PCAPS-IP 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. 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. 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. 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. 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 of the USPTO adhere to the USPTO Records Management Office's Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citation.

☐	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: _ OEDIS: Attorney/Agent applicants who complete the Application for Registration form (PTO-158) are presented a Privacy Act statement and are notified of the routine uses of their voluntarily submitted PII. OEDIS: https://www.uspto.gov/sites/default/files/documents/PTO158_Application_for_Registration.pdf ESTTA: Applicants applying for Trademark Appeals are presented with a privacy policy statement as follows: https://estta.uspto.gov/ TTAB: see appendix A	
☐	Yes, notice is provided by other means.	Specify how:
☐	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: OEDIS: Attorneys/Agents who desire to practice patent law for intellectual property protection before the USPTO must provide the required information in order for their registration to be processed. At which time the applicant may opt to

		decline to provide such information. 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. They may decline to provide PII by not submitting a trademark registration for processing.

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: OEDIS: On the PTO158 form a registering Attorney/Agent applicant is notified of consent to use of their PII. ESTTA: Trademark applicants are provided the privacy policy statement during registration and are made aware of consent to the use of their PII.

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: OEDIS: During the online registration process the Attorney/Agent are allocated the opportunity to ensure information accuracy. After registration Attorney/Agent is also provided USPTO administrative points of contact to coordinate registrant information updates. 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.

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: 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*.
☒	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): 8/3/2022 ☐ 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): PTO 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).*

Personally Identifiable Information 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 authorize 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 Network and Security Infrastructure (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."

☒	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 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/PAT-TM 6: Parties Involved in Patent Interference Proceedings. COMMERCE/DEPT-5: Freedom of Information Act and Privacy Act Request Records COMMERCE/DEPT-14, Litigation, Claims, and Administrative Proceeding 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: Enrollment Examination: N1-241-09-1: b4.1 Enrollment and Discipline Application and Roster Maintenance Files: N1-241-09-1: b4.2 Subject Files Related to Enrollment and Discipline: N1-241-09-1: b4.3 Enrollment Examination Answer Sheets – Unsuccessful Applicants: N1-241-09-1: b4.4 Administrative Law Files, Office of Enrollment and Discipline Appeal Case Files: N1-241-09-1: b4.5 Enrollment Examination Answer Sheets – Successful Applicants: N1-241-09-1: b4.6 Enrollment and Discipline Roster of Attorney's and Agents Registered to Practice Before the USPTO: N1-241-09-1: b4.7 Director's OED Decision Files: N1-241-09-1: b4.8 FOIA, Privacy Act, and classified documents administrative records: GRS 4.2:001 Access and disclosure request files: GRS 4.2:020
☐	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: 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.
☒	Quantity of PII	Provide explanation: The quantity of PII in this system 100,000s, enough to warrant adequate protection.
☒	Data Field Sensitivity	Provide explanation: The combination of name, proprietary business information, etc. can make the data fields more sensitive.
☒	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.
☒	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.
☒	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.
☐	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.

☐	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.

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.

Points of Contact and Signatures

System Owner
Name: Diane Park
Office: Office of the Chief Information Officer (OCIO)
Phone: (571) 272-5332
Email: Diane.Park@uspto.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: Users, Park, Diane Digitally signed by Users, Park, Diane Date: 2022.09.19 18:28:36 -04'00'

Date signed: _____

Chief Information Security Officer
Name: Don Watson
Office: Office of the Chief Information Officer (OCIO)
Phone: (571) 272-8130
Email: Don.Watson@uspto.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: Users, Watson, Don Digitally signed by Users, Watson, Don Date: 2022.10.04 09:13:04 -04'00'

Date signed: _____

Privacy Act Officer
Name: Ezequiel Berdichevsky
Office: Office of General Law (O/GL)
Phone: (571) 270-1557
Email: Ezequiel.Berdichevsky@uspto.gov

I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA.

Signature: Users, Berdichevsky, Ezequiel Digitally signed by Users, Berdichevsky, Ezequiel Date: 2022.09.30 08:27:22 -04'00'

Date signed: _____

Bureau Chief Privacy Officer and Authorizing Official
Name: Henry J. Holcombe
Office: Office of the Chief Information Officer (OCIO)
Phone: (571) 272-9400
Email: Jamie.Holcombe@uspto.gov

I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.

Signature: Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry Date: 2022.10.04 14:41:10 -04'00'

Date signed: _____

Co-Authorizing Official
Name: N/A
Office: N/A
Phone: N/A
Email: N/A

I certify that this PIA accurately reflects the representations made to me herein by the System Owner, the Chief Information Security Officer, and the Chief Privacy Officer regarding security controls in place to protect PII/BII in this PIA.

Signature: _____

Date signed: _____

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.