Version Number: 01-2019

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

Jennifer Goode 11/08/2020

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 description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

(a) Whether it is a general support system, major application, or other type of system
IPLMSS is a master Automated Information System (AIS) which facilitates grouping and management of 11 separately bounded AISs 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 (PTAB); Office of Patent Training (OPT); and Office of Policy and International Affairs (OPIA).

(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)
The Intellectual Property Leadership Management Support System (IPLMSS) is a master AIS that interconnects with the following separately accredited USPTO master AIS;

Trademark Processing System - Internal Systems (TPS-IS) – PTOT-003-00 consists of several applications that are used in the automated processing of trademark applications.

PCAPS-IP Patent Capture and Application Processing System - Capture and Initial Processing (PCAPS-IP) – PTOP-006-00 consists of several applications that facilitate the automated processing of patent applications.

Patent Capture and Application Processing System - Examination Support (PCAPS-ES) – PTOP-005-00 consists of several applications that enable patent examiners and public users to search and retrieve application data and images and patent examiners and patent applicants to identify individuals and organizations with intellectual property, pre-grant, and published applications.

Patent Trial and Appeal Board Center (PTAB-Center) – PTOP-010-00 is an AIS that is used to support the conduct of trials, including inter partes, post-grant, and covered business method patent reviews and derivation proceedings, the hearing of appeals from adverse examiner decisions in patent applications and reexamination proceedings, and the rendering of decisions in interferences.

Agency Administrative Support System - (AASS) – PTOC-002-00 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.

Fee Processing Next Generation (FPNG) – PTOC-004-00 provides a modern payment system to the public and internal facing functionality that enables USPTO employees to support customers

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

The Intellectual Property Leadership Management Support System (IPLMSS) is a master system that containerizes 11 separately bounded Automated Information Systems (AIS) that support USPTO internal and external users by providing the capability to manage, search, and retrieve information and documents.

The 11 separately bounded Automated Information Systems (AIS) that support (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 (PTAB); Office of Patent Training (OPT); and Office of Policy and International Affairs (OPIA) are as follows:

Trademark Trial and Appeal Board VUE (TTABVUE) – PTOL-001-11 is an AIS and is a System of Record. TTABVUE has internal web interfaces that facilitate TTAB staff with internal information sharing and administrative matters. TTABVUE's public facing website provides the public with a means to perform searches of publicly releasable TTAB proceeding files by proceeding number, application number, registration number, mark, party, or correspondent. The publicly available proceedings do not allow the public to view any confidential content. Public releasable information is posted via the normal processing of board proceedings using TTAB's internal system, TTABIS, and/or via a submission filed from ESTTA. Information may be used in litigation.

Electronic Freedom of Information Act (E-FOIA) - PTOL-001-01 is an AIS and a System of Record that provides transparency of the agency's decisions and information to the public in support of FOIA and/or Privacy requests. E-FOIA allows the public to perform FOIA queries to verify FOIA request status information only. The content within the E-FOIA system may include public and non-public releasable decision documents (BII) relating to patent applications. Only publicly releasable documents are made available to the public. Also, the E-FOIA system includes a number of public-facing document libraries (aka, online FOIA Reading Rooms) whereby the public can browse to view publicly releasable OGC, PTAB, TTAB, and other decisions and documents of interest to the public. Information may be used in litigation.

Electronic System for Trademark Trials and Appeals (ESTTA) - PTOL-001-03 is an AIS and not a System of Record that supports administrative matters by providing the public with an online website to submit all filings to the Trademark Trial and Appeal Board

(TTAB). Some information submitted may contain confidential BII. All of the information posted on this site is available to the public. Information may be used in litigation.

Freedom of Information Act Electronic Management System (FEMS) - PTOL-001-04 is an AIS and System of Record that supports the end to end processing of FOIA and Privacy Act requests from the public. FEMS automatically updates the status of the FOIA/Privacy requests as they proceed through the internal workflow processes. Public users use the E-FOIA AIS to view status of previously submitted FOIA request. Information is not used in litigation.

General Counsel Case Tracking System (GCCTS) - PTOL-001-05 is an internal legal practice management AIS and a System of Record that is used in administrative matters for docketing intellectual property cases and for managing documents and contacts. GCCTS may contain some sensitive PII. GCCTS is only accessible to authorized internal Office of the Solicitor users. Information may be used in litigation.

General Counsel Library System (GCLS) - PTOL-001-06 is an AIS and not a System of Record. GCLS is internally accessible to USPTO's Office of the General Counsel (OGC) and Office of Policy and International Affairs (OPIA) authorized users only. GCLS is used to manage the library's bibliographic catalogs of non-sensitive hardback or softback resource reference materials (i.e., federal codes, federal statutes, legal treatises, etc.). GCLS facilitates creation, updates and deletion of borrower catalog records and book order tracking. There is no PII/BII and may be used in litigations.

Office of Enrollment and Discipline Item Bank (OEDIB) – PTOL-001-08 is not a System of Record but an internally accessible web-based COTS AIS that authorized users in OED and OPT use to administer the examination questions item banks (i.e., repository updates, test creation, test grading, report generation and assessment delivery to participants, etc.) for patent practitioners, patent examiners and patent managers. Access to the examination answers are restricted since the assessments are used to validate patent practitioners, patent examiners and patent managers' qualifications. There is no PII/BII and is not used in litigations.

Office of Enrollment and Discipline Information System (OEDIS) – PTOL-001-09 is an AIS and is a System of Record that is used for administrative matters. OEDIS consists of OEDIS Core and OEDIS CI (Customer Interface). OEDIS Core is used internally by OED to process patent practitioner registration, maintain the practitioner roster and monitor practitioner investigative and disciplinary actions. OEDIS CI supports sharing information by enabling the public to submit registrations and allowing the public to browse and search the official roster of registered patent attorneys and agents. Content within OEDIS may include sensitive PII (i.e., name, phone number, mailing/email address, birthdate, citizenship, place of birth, education, reasonable accommodation information, and alien registration information) and there may be instances where it is required or authorized by law (e.g., FOIA/Privacy Act request) to be judiciously shared with only authorized parties. Information may be used in litigation.

Trademark Trial and Appeal Board Information System (TTABIS) – PTOL-001-10 is an internally integrated AIS and not a System of Record that supports the administrative activities of the TTAB: workflow processes, proceedings, proceeding status, generated actions, tracking of record data and report issuance. The system is web-based and accessed by authorized internal TTAB users only. Information is shared to the public through the customer service center by tracking and analyzing information and case requests from the public. Information may be used in litigation.

e-Discovery Software Suite (EDSS) - PTOL-001-14 is an internally managed COTS web-based AIS and not a System of Record that is restricted to authorized OGC users for administration of litigation holds and processing Electronically Stored Information (ESI). The system provides legal staff with functions for e-Discovery filtering, tagging, document redaction, document reviews, and preparing the ESI for production in a legal case. EDSS content may include sensitive PII/BII and there may be instances where it is required by law (e.g., FOIA/Privacy Act or e-Discovery requests) to be shared only with authorized parties. Information may be used in litigation.

Notice of Suit Processing System (NOSPS) – PTOL-001-13 is an internal web-based AIS and not a System of Record that supports OGC. NOSPS is not a System of Record. The system is restricted to OGC administrative users that scan and perform data entry on Notice of Suit documents received in the mail from the U.S. District Courts where suits are filed in cases relating to a Patent or Trademark. The system routes a copy of each processed notice to the respective Patent and Trademark electronic application files and provides a reporting capability for counts and status. Information may be used in litigation.

(e) How information in the system is retrieved by the user
The general public may retrieve public releasable information from the following AIS public websites: TTABVUE, ESTTA, E-FOIA and OEDIS (CI).

(f) How information is transmitted to and from the system
IPLMSS internet/intranet services are web based and all communications are secured via end-to-end transport layer protocols.

(g) Any information sharing conducted by the system
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 § 552 [FOIA requests, EFOIA decisions],
5 USC § 552a [Privacy 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 (version 01-2015).
☒ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2017 or later).

Section 2: Information in the System

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

Identifying Numbers (IN)					
a. Social Security*	☒	f. Driver's License	☒	j. Financial Account	☒
b. Taxpayer ID	☒	g. Passport	☒	k. Financial Transaction	☒
c. Employer ID	☒	h. Alien Registration	☒	l. Vehicle Identifier	☐
d. Employee ID	☒	i. Credit Card	☒	m. Medical Record	☐
e. File/Case ID	☒				
n. Other identifying numbers (specify):					

*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form: For EDSS or FEMS; the SSN may be incidentally collected as a result from either e-Discovery, FOIA or
Privacy Act search requests of agency records.

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. Physical Characteristics	☒
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	☒		
d. Work Telephone Number	☒	h. Employment Performance Ratings or other Performance Information	☐		
k. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	☐	d. Photographs	☒	g. DNA Profiles	☐
b. Palm Prints	☐	e. Scars, Marks, Tattoos	☐	h. Retina/Iris Scans	☐
c. Voice Recording/Signatures	☒	f. Vascular Scan	☐	i. Dental Profile	☐
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	☒	c. Date/Time of Access	☒	e. ID Files Accessed	☐
b. IP Address	☒	d. Queries Run	☒	f. Contents of Files	☐
g. Other system administration/audit data (specify):					

Other Information (specify)
Reasonable accommodation data

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 EMSO 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):			

☒	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 only 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.

[EFOIA] The BII content within the E-FOIA system may include public and non-public releasable decision documents (BII) relating to patent applications. There is no sensitive PII. The information may reference federal employees, members of the public and foreign nationals.

[OEDIS] The sensitive 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.

[FEMS] The sensitive PII collected PII/BII are incidental content that may include some or all references in Section 2.1 for IN, GPD, and WRD from agency records to facilitate communications between the agency and the FOIA/Privacy Act requestor. During the course of a FOIA/Privacy Act request search, sensitive PII may be incidentally collected from agency records. Sensitive PII can be either digitally and/or manually redacted, withheld or deleted. The collected information from agency records (as part of the FOIA/Privacy requests) may be judiciously disseminated as required by law. The public correspondence PII may reference federal employees.

[GCCTS] The stored sensitive 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 and foreign nationals.

[ESTTA] collects sensitive PII (i.e., name, phone number, mailing/email address, citizenship) and/or confidential information (i.e., past business revenue) as a result from Trademark online submissions from the public. The information may reference federal employees, members of the public and foreign nationals.

[TTABIS] The sensitive PII (i.e., name, phone number, mailing/email address, citizenship) and/or confidential information (i.e., past business revenue) and confidential information (i.e., past business revenue) that is maintained and used for Trademark Trial and Appeal Board to

support decision making. TTABIS also maintains public correspondence PII (i.e., name, telephone number, mailing and/or email address). The information may reference federal employees, members of the public and foreign nationals.

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

GCLS – No PII/BII.
NOSP – No PII/BII.
OEDIB – No PII/BII

5.2 Describe any potential threats to privacy 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 is a risk and USPTO has policies, procedures and training to ensure that employees are aware of their responsibility of protecting sensitive information and the negative impact to 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. 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 (OCIO-POL-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.

Section 6: Information Sharing and Access

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

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	☒	☐	☒
DOC bureaus	☒	☐	☐
Federal agencies	☒	☐	☐
State, local, tribal gov't agencies	☒	☐	☐

Public	☒	☐	☐
Private sector	☐	☐	☐
Foreign governments	☐	☐	☐
Foreign entities	☐	☐	☐
Other (specify):	☐	☐	☐

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

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

☒	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: All user access is governed by a role based and need-to-know basis that is either Active Directory or Role Base Access Control (RBAC) enforced. IPLMSS implements secure network communications with the TPS-IS, PCAPS-IP, PCAPS-ES, AASS, FPNG, PTAB-Center via end-to-end transport layer protocols and where applicable data-at-rest encryption. All IPLMSS communications are within USPTO's secured perimeter, which is protected through the Network and Security Infrastructure (NSI) and monitored by the Enterprise Monitoring and Security Operations (EMSO) systems.
☐	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

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

Class of Users			
General Public	☒	Government Employees	☒
Contractors	☒		
Other (specify):			

Section 7: Notice and Consent

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

☒	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.
☒	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement

	and/or privacy policy can be found at: https://www.uspto.gov/privacy-policy	
☒	Yes, notice is provided by other means.	Specify how: 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/ **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.*
☐	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: 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.
☐	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

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

☒	Yes, individuals have an opportunity to	Specify how:

	consent to particular uses of their PII/BII.	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.
☐	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

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

☒	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: 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.
☐	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

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

☒	All users signed a confidentiality agreement or non-disclosure agreement.
☒	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
☒	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
☒	Access to the PII/BII is restricted to authorized personnel only.
☒	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: 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 sensitive PII/BII after administrative vetting to confirm the employee requires access based on a need-*to-know*.
☒	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 9/11/2019 ☐ 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 supporting 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 ownership rights over data including PII/BII.
☐	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
☐	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

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. E-FOIA employs application logic to protect against releasing BII to the public. FEMS has technical capabilities to redact BII prior to public release. 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 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

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

☒	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: COMMERCE/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 Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.
(The PII Confidentiality Impact Level is not 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 levels. *(Check all that apply.)*

☒	Identifiability	Provide explanation: Data fields captured in the PIA include PII; such as name; gender; age; ethnicity; date and place of birth; home or work address and telephone number; home or work email address; social security numbers; taxpayer, employer, employee, file or case ID; driver's license; passport; alien registration; credit card; financial or medical information; education; occupation, job title, salary, associates or work history; and Distinguishable Features/Biometrics and BII (i.e., confidential patent application decisions).
☐	Quantity of PII	Provide explanation:
☐	Data Field Sensitivity	Provide explanation:
☒	Context of Use	Provide explanation: PII is collected in order for 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 or Privacy Act requests.
☒	Obligation to Protect Confidentiality	Provide explanation: Based on the data collected USPTO must protect the PII of each individual in accordance to the Privacy Act of 1974.
☒	Access to and Location of PII	Provide explanation: Due to collection, maintaining or dissemination of PII there are policies, procedures, necessary measures implemented to ensure the confidentiality.
☐	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.)

None. Any potential threats to privacy that exist in light of the information collected, or the sources from which the information is collected, have been identified.

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.