

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



**Privacy Impact Assessment
for the
Patent Trial and Appeal Board Center (PTAB Center)**

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

CATRINA PURVIS Digitally signed by CATRINA PURVIS
Date: 2020.10.15 14:59:49 -04'00'

09/30/2020

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

Date

U.S. Department of Commerce Privacy Impact Assessment USPTO Patent Trial and Appeal Board Center

Unique Project Identifier: PTOP-010-00

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

PTAB Center is a major application.

(b) System location

600 Dulany Street, Alexandria, VA 22314

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

PTAB Center is not a standalone system. It also interconnects with the following Major Applications:

Enterprise Software Services (ESS) is a collection of applications that centralizes common business applications and tools for modeling how the agency functions, assists with unique application development, improves business logic and support, and improves communications and collaboration within the agency.

Patent Capture and Application Processing System – Internal Support (PCAPS-IP) is a master system that is comprised of multiple Automated Information Systems that perform specific functions which includes patent submissions, patent categorization, metadata capture, and patent examiner assignment of patent applications. PCAPS-IP users include both internal USPTO personnel as well as the public.

Patent Capture and Application Processing System - Examination Support (PCAPS-ES) is a master system that enables patent examiners and public users to search and retrieve application data, images, and patent applicants in order to identify individuals and organizations with intellectual property, pre-grant, and published applications.

Patents End-to-End (PE2E) is a Master system portfolio consisting of next generation Patent Automated Information Systems (AIS) with a goal creating a single web-based examination tool, which provides users with unified and robust interface that does not require launching of separate applications in separate windows.

Intellectual Property Leadership Management Support Systems (IPLMSS) is a master Automated Information System (AIS) which facilitates grouping and managing 11 general support and 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).

Fee Processing Next Generation (FPNG) - is a master system that provides a payment method to the public and internal facing functionality that enables USPTO employees to support customers.

Agency Administrative Support System (AASS) is a master system that supports multiple enterprise administrative functions. Enables the Under Secretary of Commerce for Intellectual Property and Director of the USPTO to receive and respond to a wide range of official correspondence by electronically capturing routing and tracking both incoming and responding documents. As an automated document management system supports the Office of Policy and International Affairs (OPIA) with the capabilities of capturing, indexing, searching and retrieving the documents. Provide the Chief Economist's office with a solution to store data and perform statistical analysis in a secured environment.

Information Delivery Product (IDP) is a master system that provides access to integrate USPTO data through various tools in support of not only reporting and visualizing but also analytics used in decision-making across USPTO.

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

PTAB Center is a major application for supporting USPTO's administrative law body Patent Trial and Appeal Board (PTAB) for the purpose of electronically filing documents in connection with Inter Partes Review (IPR), Covered Business Method Patents (CBM), Post Grant Review (PGR), and Derivation Proceedings (DER) established under the Leahy-Smith America Invents Act (AIA). It is also used for the administrative processing of pre-Grant Appeals of certain types of adverse decisions by patent examiners. Appeals documents are stored in P-ELP (Patents content management system) and the statuses are recorded for the cases in the Appeals database. The addresses of the Appellants are stored in PALM and the Appeals database does not store the addresses. PTAB Center also updates PALM on transaction codes. The Appeals database records only the transactions pertaining to the Appeal processing by the PTAB. This database is only used for Appeal processing by internal PTAB Users; it is not used or accessible to the public. In addition, PTAB Center provides case management, case tracking and notification, hearing schedule, data analytics and reporting capabilities, data search and search results, data integration, data synchronization, and data store, document submission and management, workload balance and management and electronic records management.

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

As internal users, PTAB Administrators have access to the new cue of petitions for assignment. They are able to see certain attributes of the available judges so they can properly and accurately assign petitions to the appropriate judge.

As internal users, Supervisory Paralegals and some Paralegals have access to the Import Manager screens to automatically import Appeal cases into PTAB Center. They also have access to the Post Decisional Case Management screen to view recently decided cases.

As internal users, Judges have access to all the available petitions that they are assigned to or given permission to access. In addition, Judges and Patent Attorneys have ‘case dockets’ that they can view with all the cases that are assigned (Paralegals do not). All internal users have ‘assignment dockets’ for tasks they are assigned.

Public (External) users can review/search the PTAB Center documents/filings/proceedings without logging in to the system. Public user can search by ‘AIA Review Number, Patent Number, Application Number, Party Name, AIA Review/Case Type, and Tech Center.’, Public users have read only access to the documents. Public users create their own account from the PTAB Center website by clicking on ‘Create an Account’ for the following actions: *“Person or group who challenges the validity of the AIA proceedings. Person or group who has or claims to have the ownership of the AIA proceeding. Patent application or Owner who is appealing a final office decision. Applicants or Patent Owners involved in challenge over inventor-ship. Persons or groups, other than the Patent Owner/Appellant or the public, who actively participate in the validity challenges of proceeding”*.

A public user is required to provide First Name, Last Name, Phone Number and Email Address. Additionally, the public user is also required to create a password in the ‘Register a New Account Form’. After the user clicks on ‘Register’, an email is sent out by the system to the user with instructions and a link to validate/activate the account. When the user clicks on the provided link, a screen with validation code is displayed, user clicks on submit, account is activated and a message ‘You’ve successfully registered for PTAB Center!’ is displayed.

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

PTAB Center implements cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission. For external facing systems HTTPS and TLS 1.2 or higher, AES with 256-bit encryption, RSA with 2048-bit exchange as key exchange mechanism are used. However, for SSL usage, all activities are internal to USPTO and per OMB M-15-13, internal use of HTTPS is encouraged but not

required.

(g) *Any information sharing conducted by the system*

Yes,

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

5 U.S.C. 301, 44 U.S.C. 3101, 35 U.S.C. 134, 135, 311-318, and 321-328.

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

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

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

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	<input type="checkbox"/>	d. Photographs	<input type="checkbox"/>	g. DNA Profiles	<input type="checkbox"/>
b. Palm Prints	<input type="checkbox"/>	e. Scars, Marks, Tattoos	<input type="checkbox"/>	h. Retina/Iris Scans	<input type="checkbox"/>
c. Voice Recording/Signatures	<input type="checkbox"/>	f. Vascular Scan	<input type="checkbox"/>	i. Dental Profile	<input type="checkbox"/>
j. 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 checked="" type="checkbox"/>
b. IP Address	<input checked="" type="checkbox"/>	d. 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 type="checkbox"/>	Hard Copy: Mail/Fax	<input type="checkbox"/>	Online	<input checked="" type="checkbox"/>
Telephone	<input type="checkbox"/>	Email	<input type="checkbox"/>		
Other (specify):					

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

Non-government Sources					
Public Organizations	<input type="checkbox"/>	Private Sector	<input checked="" 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.

The non-privileged users of PTAB Center are prevented from executing privileged functions by the concept of least privilege. Only administrators, have access to privileged functions. Access to privileged functions is approved by the Technical Lead or business unit before assigning to administrators. Additionally, integrity verification to detect unauthorized changes to include Windows log transfer configuration, Unix syslog parameters, NTP values, SNMP values, local admin accounts, user groups, and client parameters monitoring are done at EUS, EWS and EMSO interconnected systems levels.

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. 0651-0063 PTAB Actions 0651-0069 Patent Review and Derivations
<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 (TUCPBNPD)			
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):			

<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 type="checkbox"/>
For litigation	<input 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 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): For correspondence (by email) purposes and to review the progress of the petition. To run internal reports to be used by USPTO business unit.			

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).

PTAB Center enables the public (registered or anonymous) to search for AIA reviews by the party name, AIA Review/Case type, patent number or application number, PTAB proceedings and documents related to proceedings. PTAB Center also provides this public data as bulk downloads. PTAB Center collects, maintains and disseminates data that may contain the following types of public PII (U.S. and foreign):

Patent applicant PII (i.e., applicant's name, correspondence address, email, telephone number) which is of a public nature to facilitate the patent application process or correspondence between the patent applicant and USPTO.

Federal employee PII (i.e. employee name, email, telephone number and USPTO official mailing address) which is used externally for correspondence to the patent applicant(s) and internally for USPTO business unit's reports.

PTAB Center business unit conducts post-grant petition Trials and pre-grant Appeals. These include inter Partes disputes, covered business method patent reviews and derivation proceedings; hearing appeals from adverse examiner decisions in patent applications and reexamination proceedings; and rendering decisions in interferences. Public PII may be contained within these internal business processes.

PTAB Center does access BII (i.e., unpublished patent applications) stored on Patent Capture and Application System –Examination Support (which is approved for PII/BII); however PTAB Center does not store, collect or disseminate 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.)

Potential threats to privacy include unauthorized access and unauthorized changes to information which includes non-sensitive Personally Identifiable Information (PII). PTAB Center handles and retains both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. Only people authorized to access the system are allowed to handle the information or access the information retained within the system. PTAB Center also uses access control mechanisms implemented on all of its components to ensure the information is handled and retained in accordance with all applicable laws and requirements. System records are retained in accordance with National Archives and Records Administration approved records control schedules. PTAB Center is used to support determinations in inter-partes disputes. Only limited internal PTAB users have access to an assigned dashboard and their work queue and are able to view petitions. Judges have access to petitions that they are assigned to or have been given permission to access.

Until petitions are final, petitions are accessible only to limited internal users. After petitions are final, these become public documents. Printing is done by authorized users only; printed documents are picked up as soon as documents are printed. Information is not disposed of except in accordance with applicable record control schedules. Additionally, the system owner is responsible for ensuring that the PTAB Center is deployed and operated in accordance with the agreed-upon security controls, that the support personnel receive requisite security training, and that necessary resources are available for the Security Authorization processes.

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 type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DOC bureaus	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Federal agencies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
State, local, tribal gov't agencies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Private sector	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign governments	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign entities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other (specify):	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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.

<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>Patent Capture and Application System – Examination Support (PCAPS-ES) BII (unpublished patent applications) are managed and secured by the USPTO's Active Directory (AD) and Unix Enterprise.</p> <p>Patent Capture and Application Processing System – Internal Support (PCAPS-IP) – published patent images may be retrieved.</p> <p>Intellectual Property Leadership Management Support Systems (IPLMSS) – only PTAB judge counsel verification is shared.</p> <p>Fee Processing Next Generation (FPNG) – No personal financial information is retrieved only applicant/parties payment status.</p> <p>The technical access controls are securely managed through Active Directory and Enterprise Unix permission enforcements. Although PTAB interconnects with other USPTO master systems authorized to process PII/BII, PTAB does not retrieve any sensitive PII/BII from those systems. There are infrastructure and other OCIO established technical controls and administrative policies, which include password authentication at the server and database levels. HTTPS/TLS is used for all data transmissions to and from the Internet, USPTO DMZ, and PTOnet. A dedicated socket is used to perform encryption and decryption and where appropriate data at rest encryption is leveraged.</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.

6.3 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	<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"/>	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: http://www.uspto.gov/privacy-policy	
<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.	Specify why not: Without providing name, email address, address and telephone number, petition cannot be filed, submitted and reviewed.

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.	Specify why not: Individuals must volunteer to provide their name, email, correspondence address, phone number in order to file petitions for review.

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.	Specify how: Users can login to their accounts and update the information.
<input type="checkbox"/>	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.)*

<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"/>	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Although PTAB does not store, maintain, process sensitive PII/BII, system monitoring is enabled by default to send system and security logs to the OCIO Command Center (C3), who review and analyze system logs for inappropriate or unusual activities.

<input checked="" type="checkbox"/>	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 09/13/2019 <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
<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 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).
<input checked="" type="checkbox"/>	A security assessment report has been reviewed for the supporting 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 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 type="checkbox"/>	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).*

In accordance with NIST 800-18 Rev. 1 and NIST 800-53 Rev. 4, the PTAB Center System Security Plan (SSP) addresses the extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment. The SSP is reviewed on an annual basis. In addition, annual assessments and Continuous Monitoring reviews are conducted on the PTAB Center data. The USPTO Office of Policy and Governance/Cybersecurity Division (OPG/CD) conducts these assessments and reviews based on NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations and NIST SP 800-53A Revision 4 Assessing Security and Privacy Controls in Federal Information Systems and Organizations. The results of these assessments and reviews are documented in the PTAB Center Security Assessment Package as part of the system’s Security Authorization process.

Management Controls

USPTO uses the Life Cycle review process to ensure that management controls are in place for PTAB Center. During the enhancement of any component, the security controls are reviewed, re-evaluated, and updated in the System Security Plan. The System Security Plan specifically addresses the management, operational, and technical controls that are in place, and planned, during the operation of the enhanced system. Additional management controls include performing national agency checks on all personnel, including contractor staff. Additionally, USPTO develops privacy and PII-related policies and procedures to ensure safe handling, storing, and processing of sensitive data.

Operational Controls

Automated operational controls include securing all hardware associated with the PTAB Center in the USPTO Data center. The Data Center is controlled by access card entry, and is manned by a uniformed guard service to restrict access to the servers, their Operating Systems and databases.

Technical Controls

PTAB Center is secured by various USPTO infrastructure components, including the Network and Security Infrastructure (NSI) system and other OCIO established technical controls to include password authentication at the server and database levels. Web communications leverages modern encryption technology such as TLS over HTTPS. Dedicated interconnections offer protection through IPsec VPN tunnels. PTAB Center PII/BII is encrypted.

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."

<input checked="" type="checkbox"/>	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number <i>(list all that apply)</i> : Parties Involved in Patent Interference Proceedings--PAT/TM-6; Litigation, Claims, and Administrative Proceeding Records--COMMERCE/DEPT-14; Attorneys and Agents Registered or Recognized to Practice Before the Office--PAT/TM-1; Users of Public Facilities of the Patent and Trademark Office--PAT/TM-14; Patent Application Files--PAT/TM-7
<input 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.)*

<input checked="" type="checkbox"/>	There is an approved record control schedule. Provide the name of the record control schedule: Refer to: http://ptoweb.uspto.gov/ptointranet/cisd/cio/records_mgmt/docs/Appendix%20A%20-%20USPTO%20Functional%20Records%20Schedules%20By%20Bucket%20and%20Citation.pdf N1-241-10-1:7.4 Patent Legal Correspondence N1-241-09-1:b2.1 Patent Interference Cases – Open to the Public N1-241-09-1:b2.3 Patent Appeal Cases N1-241-09-1:b2.6 Patent Appeal and Interference Case Tracking
<input type="checkbox"/>	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:
<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 type="checkbox"/>	Overwriting	<input type="checkbox"/>
Degaussing	<input type="checkbox"/>	Deleting	<input type="checkbox"/>
Other (specify): No disposal			

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.)

<input checked="" 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 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 levels. *(Check all that apply.)*

<input checked="" type="checkbox"/>	Identifiability	Provide explanation: Public users enter PII (name, home/business address, email address, and telephone number) online to file petition
<input checked="" type="checkbox"/>	Quantity of PII	Provide explanation: There are an estimated ~200k records comprised of ~50k petitions and affiliated attorney actions. Since attorneys are involved in multiple cases, the actual number of records with unique PII will be less than ~200k.
<input type="checkbox"/>	Data Field Sensitivity	Provide explanation:
<input type="checkbox"/>	Context of Use	Provide explanation:
<input type="checkbox"/>	Obligation to Protect Confidentiality	Provide explanation:
<input checked="" type="checkbox"/>	Access to and Location of PII	Provide explanation: The information captured, stored, and transmitted by the PTAB-Center system is accessible by internal USPTO users. Some of the information is also available to the public and may contain PII, such as Decision documents and Powers of Attorney.
<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.)

Potential threats to privacy include unauthorized access and unauthorized changes to confidential and sensitive information, which includes Personally Identifiable Information (PII). In order to combat this threat, PTAB Center is configured to send system and security logs to the OCIO Command Center (C3), whose administrators review and analyze the logs generated in real time for any inappropriate or unusual activities, such as unauthorized system access, unauthorized remote access, or unauthorized configuration settings change, on a daily basis, and report any findings of inappropriate or unusual activity to authorized PTAB Center personnel such as the System Owner Administrators or Technical Leads. If there is any inappropriate or unusual activity, PTAB Center authorized personnel will create a CRQ and take appropriate action to address these activities. Additionally, administrators may adjust the level of review, analysis and reporting if there is a change in the risk to organization assets or operations based on law enforcement information, intelligence information or other credible sources of information.

Furthermore, PTAB Center documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII. Additionally, USPTO conducts Privacy Threshold Analysis (PTA) and Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures. PIA identifies the privacy risks to information systems and how those risks are mitigated by restricting access control and the sharing PII with other systems and Organizations. PTAB Center identifies PII to be collected and used and the PII disposal process, which is documented in PIA.

PTAB Center also provides automated mechanisms to utilize and retain the PII, which is processed by the system. In addition, the Perimeter Network (NSI) and EMSO provide additional automated transmission and monitoring mechanisms to ensure that PII information is protected and not breached by any outside entities. PTAB Center uses encryption to encrypt data in transition. Access to PII information is restricted to authorized personnel only. PII information is encrypted and stored in blob (column in Oracle database). PII information (Name, Email Address, telephone number and address) are accessible only to Judges and registered users who file a petition until petition becomes a public document.

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.