Version Number: 01-2019

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

Privacy Threshold Analysis
for the
Patent Trial and Appeal Board Center
(PTAB Center)

U.S. Department of Commerce Privacy Threshold Analysis

USPTO Patent Trial and Appeal Board Center (PTAB Center)

Unique Project Identifier: PTOP-010-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description system (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

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 boundaried 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. Provides 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 purpose that the system is designed to serve

PTAB Center is used 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.

e) The way the system operates to achieve the purpose

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.

f) A general description of the type of information collected, maintained, use, or disseminated by the system

First Name, Last Name, E-mail address, Telephone Number of Public Users who file petitions.

g) Identify individuals who have access to information on the system

Authorized Administrators, Judges, Supervisory Paralegals, Paralegals, Patent Attorneys, and Hearings Team.

h) 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.

i) 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.

Questionnaire:

1. What is the status of this information system?

☐ This is a new information system. *Continue to answer questions and complete certification.*

☐ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

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. *Continue to answer questions and complete certification.*

☐ 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). *Continue to answer questions and complete certification.*

☒ 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). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

☐ Yes. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

☒ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

☐ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

☒ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate personally identifiable information

(PII)?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

☒ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

- ☐ DOC employees
- ☐ National Institute of Standards and Technology Associates
- ☐ Contractors working on behalf of DOC
- ☐ Other Federal Government personnel
- ☒ Members of the public

☐ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

☐ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
Provide the legal authority which permits the collection of SSNs, including truncated form.

☒ No, the IT system does not collect, maintain, or disseminate SSNs.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

☒ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

☐ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

☐ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

☒ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

☒ I certify the criteria implied by one or more of the questions above **apply** to the Patent Trial and Appeal Board Center (PTAB Center) and as a consequence of this applicability, I will perform and document a PIA for this IT system.

☐ I certify the criteria implied by the questions above **do not apply** to the Patent Trial and Appeal Board Center (PTAB Center) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO): Ajai Viswambharan

Signature of SO: Users, Viswambharan, Ajai Digitally signed by Users, Viswambharan, Ajai Date: 2020.07.08 09:28:23 -04'00' Date: _____

Name of Privacy Act Officer (PAO): John Heaton

Signature of PAO: Users, Heaton, John (Ricou) Digitally signed by Users, Heaton, John (Ricou) Date: 2020.07.08 09:07:12 -04'00' Date: _____

Name of Chief Information Security Officer (CISO): Don Watson

Signature of CISO: Users, Watson, Don Digitally signed by Users, Watson, Don Date: 2020.07.09 14:16:19 -04'00' Date: _____

Name of Co-Authorizing Official (Co-AO) & Bureau Chief Privacy Officer (BCPO): Henry J. Holcombe

Signature of AO & BCPO: Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry Date: 2020.07.13 09:45:16 -04'00' Date: _____

Name of Co-Authorizing Official (Co-AO): Scott R. Boalick

Signature of AO: Users, Boalick, Scott Digitally signed by Users, Boalick, Scott Date: 2020.07.17 17:21:37 -04'00' Date: _____