Version Number: 01-2017

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

Privacy Impact Assessment
for the
Patent Trial and Appeal Board E2E (PTAB E2E)

Reviewed by: David Chiles, Bureau Chief Privacy Officer (Acting)

☑ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

□ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

for Dr. Catrina D. Purvis 05/20/2019

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 E2E (PTAB E2E)

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) a general description of the information in the system

The new PTAB E2E architecture will enhance case/proceeding management and reporting functions will consolidate the various types of data that PTAB is currently tracking. A number of individuals are manually collecting this data to generate a variety of reports, analytics, and case management.

The PTAB E2E is the system based on the concept of a case or a proceeding to replace the multiple systems separately dealing with America Invents Act (AIA) Trials, Interferences, Appeals, and separate spreadsheets and databases. The objective of PTAB E2E is to meet its statutory obligations under AIA, the United States Patent and Trademark Office (USPTO) Strategic Goal of Optimizing Patent Quality and Timeliness, and improving the Appeal and Post-Grant Processes. PTAB E2E formalize a solution that aligns with Patent End-to-End (PE2E) as much as feasible to meet business requirements that support a geographically dispersed workforce of Judges and Paralegals and supports all Board Trial types and appeals for 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.

(b) a description of a typical transaction conducted on the system

Create, submit and review petitions.

(c) any information sharing conducted by the system

Yes

(d) a citation of the legal authority to collect PII and/or BII

5 U.S.C. 301 and 44 U.S.C. 3101.

(e) the Federal Information Processing Standard (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.)*

☒ This is an existing information system in which changes do not create new privacy risks. *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):					

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*	□	e. File/Case ID	□	i. Credit Card	□
b. Taxpayer ID	□	f. Driver's License	□	j. Financial Account	□
c. Employer ID	□	g. Passport	□	k. Financial Transaction	□
d. Employee ID	□	h. Alien Registration	□	l. Vehicle Identifier	□
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					
*If SSNs are collected, stored, or processed by the system, please explain if there is a way to avoid such collection in the future and how this could be accomplished:					

General Personal Data (GPD)					
a. Name	☒	g. Date of Birth	□	m. Religion	□
b. Maiden Name	□	h. Place of Birth	□	n. Financial Information	□
c. Alias	□	i. Home Address	☒	o. Medical Information	□
d. Gender	□	j. Telephone Number	☒	p. Military Service	□
e. Age	□	k. Email Address	☒	q. Physical Characteristics	□
f. Race/Ethnicity	□	l. Education	□	r. Mother's Maiden Name	□

s. Other general personal data (specify):

Work-Related Data (WRD)					
a. Occupation	☐	d. Telephone Number	☒	g. Salary	☐
b. Job Title	☒	e. Email Address	☒	h. Work History	☐
c. Work Address	☒	f. Business Associates	☐		
i. 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)

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 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			
To determine eligibility	□	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): 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 E2E 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 E2E also provides this public data as bulk downloads. PTAB E2E 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 member(s) 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 E2E business unit conducts petition trials, including inter partes, post-grant, covered business method patent reviews and derivation proceedings; hears appeals from adverse examiner decisions in patent applications and reexamination proceedings; and renders decisions in interferences. Public PII may be contained within these internal business processes.

PTAB E2E 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 E2E does not store, collect or disseminate BII.

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: 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 infrastructure and other OCIO established technical controls and administrative polices, 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.
☐	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: http://www.uspto.gov/privacy-policy	
☐	Yes, notice is provided by other means.	Specify how:
☐	No, notice is not provided.	Specify why not:

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

☐	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
☒	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: 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.

☐	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
☒	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: PII information is not used by the system for any purpose, PII information is used to track petitions.

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: User can login to their accounts and update the information.
☐	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:
☒	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 01/31/2018 ☐ This is a new system.
☒	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 (POAM).
☒	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.

In accordance with NIST 800-18 Rev. 1 and NIST 800-53 Rev. 4, the PTAB E2E 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 E2E 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 E2E Security Assessment Package as part of the system's Security Authorization process.

Management Controls

1. USPTO uses the Life Cycle review process to ensure that management controls are in place for PTAB E2E. 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

1. Automated operational controls include securing all hardware associated with the PTAB E2E 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

1. PTAB E2E 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 1.1/1.2 over HTTPS. Dedicated interconnections offer protection through IPSec VPN tunnels. PTAB E2E 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."

☒	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: Litigation, Claims, and Administrative Proceeding Records--COMMERCE/DEPT-14 Parties Involved in Patent Interference Proceedings--PAT/TM-6 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
☐	Yes, a SORN has been submitted to the Department for approval on (date).
☐	No, a SORN is not being created.

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: 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
☐	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): 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.

☒	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: Public users enter PII (name, home/business address, email address, and telephone number) online to file petition
☒	Quantity of PII	Provide explanation: There are an estimated 20 thousand records comprised of 5 thousand petitions and affiliated attorney actions. Since attorneys are involved in multiple cases, the actual number of records with unique PII will be less than 20 thousand.
☐	Data Field Sensitivity	Provide explanation:
☐	Context of Use	Provide explanation:
☐	Obligation to Protect Confidentiality	Provide explanation:
☒	Access to and Location of PII	Provide explanation: The information captured, stored, and, transmitted by the PTAB-E2E system is accessible by internal USPTO users and the public. They are comprised of Decision documents (Power of Attorney).
☐	Other:	Provide explanation:

Section 12: Analysis

12.1 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.

12.2 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.