

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



**Privacy Impact Assessment
for the
Patent Capture and Application Processing System – Initial
Processing (PCAPS-IP)**

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

for Dr. Catrina D. Purvis

LISA MARTIN

Digitally signed by LISA MARTIN
Date: 2019.06.14 14:59:13 -04'00'

06/14/2019

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

Date

U.S. Department of Commerce Privacy Impact Assessment USPTO Patent Capture and Application Processing System – Initial Processing (PCAPS-IP)

Unique Project Identifier: PTOP-006-00

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.

PCAPS-IP is an Application information system, and provides support to the United States Patent and Trademark Office (USPTO) for the purposes of capturing patent applications and related metadata in electronic form, processing applications electronically, reporting patent application processing and prosecution status, and retrieving and displaying patent applications. PCAPS-IP is comprised of multiple Automated Information Systems (components) that perform specific functions, including submissions, categorization, metadata capture, and patent examiner assignment of patent applications. PCAPS-IP users include both internal USPTO personnel as well as the public.

Application Routing Tool (ART): Supports an automated system that provides a suggested routing location for new patent applications that have been successfully scanned into the Patent Application Services and Security (PASS) database. The system does not collect, process or transmit sensitive PII.

Checker (Checker): Enables public users to check sequence listings before submission to the USPTO. The Checker system validates patent applications in compliance with 37 Code of Federal Regulations (CFR) 1.821 – 1.825 for both ‘old rules’ (October 1990) and ‘new rules’ (July 1998). The system does not collect, process or transmit sensitive PII.

Enterprise Application Integration (EAI) Hub - (EAI Hub): Supports the USPTO’s e-Government strategy and provides a framework for various loosely coupled Automated Information Systems (components) to share information and services across their heterogeneous environments with minimal or no changes to the existing applications. The system does not collect, process or transmit sensitive PII.

Electronic Filing System - Web (EFS-Web): Provides a simple, safe, and secure method for e-filers to submit patent application documents as PDF files over the Internet to the USPTO. The system does collect, process or transmit sensitive PII.

Patent Application Services and Security (PASS): Provides the capability to use electronic images of patent applications to support USPTO operations. The system does not collect, process or transmit sensitive PII.

PatentIn: Allows patent applicants to generate nucleic and amino acid sequence listings. PatentIn does not connect to USPTO. The PatentIn application runs locally on the user's personal computer. The system does not collect, process or transmit sensitive PII.

Patent Application Location Monitoring Pre Examination (PALM Pre-Exam): Supports the prosecution and related administrative functions of a patent application through its life cycle, and also tracks, monitors, and reports on the prosecution status of patent applications. The system does collect, process or transmit sensitive PII.

Patent Application Location Monitoring Patent Cooperation Treaty Operations System (PCT OPS): Supports an automated, workflow-driven, client-server environment that support Patent Cooperation Treaty (PCT) patent application functions. PCT OPS works with an electronic application in an integrated desktop environment. The system does not collect, process or transmit sensitive PII.

Patent Application Location Monitoring - Reporting System (PRS): Produces many productivity and statistical reports that are crucial to the Patents Corps business operation. The PRS processes and delivers reports to Patents Corp, supporting various PALM subsystems and business areas. The system does collect, process or transmit sensitive PII.

Infrastructure Code Table – (ICT): The ICT system provides the validation of a given geographic region with a specified country, and provides a list of current countries and geographic regions. ICT provides the standard PTO country codes for patent applications. The system does not collect, process or transmit sensitive PII.

(a) Whether it is a general support system, major application, or other type of system

Major system of multiple applications

(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)

Patent Search System Primary Search (PSS-PS) is a master system that processes, transmits and stores data and images to support the data-capture and conversion requirements of the USPTO to support the USPTO patent application process.

Patent Capture and Application Processing System – Examination Support (PCAPS-ES) is a master system that provides a comprehensive prior art search capability and the retrieval of patent and related information, which comprise text and images of United States (US), European Patent Office (EPO) and Japan Patent Office (JPO) patents, US pre-grant publications, Derwent data and IBM Technical Disclosure Bulletins.

Revenue and Account Management (RAM) is master system that collects fees for various USPTO goods and services related to intellectual property and the protection of intellectual property rights.

Reed Technology and Information Services (RTIS) Patent Data Capture (PDCap)/SERCO Patent Processing System (PPS): RTIS is an off-campus contractor system that captures critical fields from applicants' applications so that they are pre-loaded into an index file to reduce examiners and public search times. SERCO PPS is a contractor system that receives information from USPTO so that inventory, identification and classification activities can be performed on patent applications.

World Intellectual Property Organization (WIPO) / Foreign Patent Offices is a United Nations (U.N.) agency charged with protecting intellectual property (IP) by working with worldwide organizations to establish international classifications.

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

EFS-Web facilitates online patent application submissions for patent examiners to administratively process towards grant/no grant decision. Web surveys are conducted semi-annually to solicit input from customers of their perception of examination quality. Checker application allows the public to check sequence listings before submission to the USPTO. The Checker application validates patent applications in compliance with the Code of Federal Regulations, which could be used in litigation proceedings.

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

PatentIn and Checker websites do not require user login and are available to the public for their application tool downloads. During EFS-Web webpage sessions, patent applicants receive acknowledgement receipts directly. All other PCAPS-IP applications are for internal user(s) who require authentication prior to application access.

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

All PCAPS-IP communications must traverse the USPTO's Network and Security System, which facilitates the communications, secure access, protective services, and network infrastructure support for all USPTO applications.

(g) Any information sharing conducted by the system

PCAPS-IP applications facilitate patent examiners collaborating internally and with our Intellectual Property international partners.

- (h) *The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information*
 35 U.S.C. 1, 35 U.S.C. 2, 35 U.S.C. 115, 35 U.S.C. 184, 35 U.S.C. 261,
- (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 a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

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

Identifying Numbers (IN)					
a. Social Security*	☐	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:					

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	☒
Third Party Website or Application	☒		
Other (specify):			

2.3 Describe how the accuracy of the information in the system is ensured.

PCAPS-IP does not perform PII verification, as it is the patent applicant's responsibility to ensure accurate contact information to facilitate correspondence between the applicant and the USPTO examiners. However, BII information is verified through the patent prosecution process.

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.
☒	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 (TUCBPNPD)			
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):			

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).

The information collected is from the public (U.S. and foreign) and Federal employees. Public data is used to file and manage Patent applications. Federal employee data is used internally for Patent examiner work, management of Federal employees, and the management of the IT systems that support the USPTO.

- 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.)

When accessing EFS-Web, patent applicants submissions could be at risk to man-in-the-middle attacks. However, EFS-Web requires all user browser communications are secured through the use of HTTPS/TLS protocols.

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: USPTO's Patent Search System Primary Search (PSS-PS); Patent Capture and Application Processing System – Examination Support (PCAPS-ES); and Revenue and Account Management (RAM): - o Information is protected through a layered security approach which incorporates the use of secure authentication, access control, mandatory configuration settings, firewalls, Virtual Private Network (VPN), and encryption, where required. Internally within USPTO, data transmission confidentiality controls are provided by PTOnet. Reed Technology and Information Services (RTIS) Patent Data Capture (PDCap)/SERCO Patent Processing System (PPS) - o External contractors from RTIS and SERCO connect through secure data transfer. No PII is shared with either system. World Intellectual Property Organization (WIPO) / Foreign Patent Offices For external data transfer to WIPO, data is transmitted across USPTO's Trilateral which is a Point-to-Point dedicated Virtual Private Network (VPN)
☐	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:
☐	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: Patent applicants are advised that information submitted to USPTO is voluntary.
☐	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 consent to particular uses of their PII/BII.	Specify how: A patent applicant's submission constitutes their consent to the use of the information for the purpose(s) stated at the time of the collection.
☐	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: During patent submission via EFS-Web, applicants have opportunities to update PII/BII data prior to final submission. After a patent submission, users must contact
-------------------------------------	---	--

		the Electronic Business Center for PII updates. All subsequent BII updates occur within PCAPS-ES system.
☐	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: Audit logs.
☒	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): <u>07/17/2018</u> ☐ 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).*

PCAPS-IP collects voluntary applicant(s) correspondence information to facilitate direct communications between the applicant(s) and the Office. PCAPS-IP applications are managed and secured by the USPTO's Active Directory (AD) and Unix Enterprise infrastructure and other OCIO established technical controls, which include password authentication at the server and database levels. HTTPS 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.

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 (<i>list all that apply</i>): Patent Application Files--COMMERCE/PAT-TM-7 http://www.uspto.gov/sites/default/files/sorn/uspto-pasorn-07.pdf USPTO PKI Registration and Maintenance System--Commerce/PAT-TM-16 http://www.uspto.gov/sites/default/files/sorn/uspto-pasorn-16.pdf
☐	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
☐	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: • Evidentiary Patent Applications N1-241-10-1:4.1 • Patent Examination Working Files N1-241-10-1:4.2 • Patent Examination Feeder Records N1-241-10-1:4.4 • Patent Post-Examination Feeder Records N1-241-10-1:4.5 • Patent Case Files, Granted N1-241-10-1:2 • Abandoned Patent Applications, Not Referenced in Granted Case File N1-241-10-1:3
☐	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: The information captured by the PCAPS-IP system could identify an individual.
☐	Quantity of PII	Provide explanation:
☐	Data Field Sensitivity	Provide explanation:
☒	Context of Use	Provide explanation: The data captured, stored, or transmitted by the PCAPS-IP system is used to process patent applications and may include sensitive information from the applicant's application.
☐	Obligation to Protect Confidentiality	Provide explanation:
☒	Access to and Location of PII	Provide explanation: The information captured, stored, and transmitted by the PCAPS-IP system is maintained within USPTO systems. No sensitive-PII is shared external to PCAPS-IP system.
☐	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.)

All PII submitted are strictly voluntary and for public use.

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.