

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



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

Reviewed by: Deborah Stephens, 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

 Digitally signed by BRIAN ANDERSON  
Date: 2026.01.06 06:11:55 -05'00'

---

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 – Capture and Initial Processing (PCAPS – IP)**

**Unique Project Identifier: PTOP-006-00**

### **Introduction: System Description**

*Provide a brief description of the information system.*

Patent Capture and Application Processing System – Capture and Initial Processing (PCAPS-IP) is a major application which supports the initial stage, once patent application is submitted to United States Patent and Trademark Office (USPTO), it will be routed to PCAPS-IP system for security review and initial patent processing of applications by USPTO.

Once any application is filed PCAPS-IP will extract essential information from the patent application such as applicant information, application title, claims and drawings. PCAPS-IP uses Optical Character Recognition (OCR) to convert any scanned text into a machine-readable format. Once all information is extracted and in a machine-readable format the patent will be classified based on the subject matter. This classification will be used to assist in assigning the patent to the appropriate patent examiner.

PCAPS-IP users are internal USPTO personnel.

There are 2 sub-systems under PCAPS-IP:

#### **Patent Application Screening and Security (PASS)**

The Patent Application Screening and Security (PASS) system provides the capability to use electronic images of patent applications to support USPTO operations. The PASS system was previously identified as Patent Application Capture and Review (PACR). PASS supports two user groups: the Office of Initial Patent Examination (OIPE) and the Licensing and Review (L&R) Group. PASS provided OCR, data extraction and verification, security screening, and application viewing, Defense Threat Reduction System Administration (DTSA) compact disk (CD) generation, Pre-Grant Publication (PGPub), Grant tape publication, and East Data Center (EDC) exports.

#### **Patent Cooperation Treaty Operations (PCT OPS)**

The Patent Cooperation Treaty (PCT) Operations (OPS) also referred as PCT Operations Workflow and Electronic Review System (POWER), system is a USPTO Automated Information System (component) designed to support an automated, workflow-driven, client-server environment that support PCT patent application functions. PCT OPS works with an electronic application in an integrated desktop environment. The PCT OPS system minimizes the movement of paper through the United States Receiving Office (RO/US) processing stream and automates the application filing process under Chapter I and Chapter II of the PCT. The PCT OPS system supports the initial receipt of an application or later-submitted papers, review of the application by PCT personnel, generation of outgoing correspondence, and

tracking of the application while it is being processed by RO/US. Case files ultimately provide information in an electronic medium that facilitates exchange with PCT Operations' principal internal customer, the USPTO Examining Corps, as well as with the World Intellectual Property Organization (WIPO), Trilateral Office partners, and the other international partners of USPTO.

Address the following elements:

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

PCAPS-IP is a major application.

*(b) System location*

PCAPS-IP is located in Alexandria, Virginia.

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

PCAPS-IP interconnects with the following systems:

**Database Services (DBS)** is an Infrastructure information system, and provides a Database Infrastructure to support the mission of USPTO database needs.

**Enterprise Windows Services (EWS)** is an Infrastructure information system, and provides a hosting platform for major applications that support various USPTO missions.

**Network and Security Infrastructure System (NSI)** is an Infrastructure information system, and provides an aggregate of subsystems that facilitates the communications, secure access, protective services, and network infrastructure support for all USPTO IT applications.

**Security and Compliance Services (SCS)** provides Security Incident and Event Management, Enterprise Forensic, Enterprise Management System, Security and Defense, Enterprise Scanner, Enterprise Cybersecurity Monitoring Operations, Performance Monitoring Tools, Dynamic Operational Support Plan, & Situational Awareness and Incident Response.

**Storage - Storage Infrastructure Managed Service (SIMS)** is USPTO storage, managed by a Storage as a Service (SaaS) provider, known as SIMS. The initial capabilities for SIMS will provide storage infrastructure support for all net new Next Gen projects. In addition to Next Gen project support there will be the migration of existing legacy storage data onto the SIMS infrastructure affecting all AISs that are currently supported by the USPTO storage infrastructure. Peraton has developed a detailed Storage Infrastructure which is designed for an extremely high level of availability, reliability, and resiliency for both block and file data

types. The Storage Infrastructure accommodates the need for the Boyers site to be an alternate processing site.

**ICAM-Identity as a Service (ICAM-IDaaS)** provides unified access management across applications and Application Programming Interface (API) based on single sign-on service. Identity and access management is provided by Okta's cloud-based solution which uses Universal Directory to create and manage users and groups.

**Fee-Processing Next Generation (FPNG)** includes fee management for external customers (Financial Manager, payment page / services, and fee services consumed by other systems) and fee management for internal customers (e.g., Fee Processing Portal for processing fees and refunds).

**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), US pre-grant publications, Derwent data, and IBM Technical Disclosure Bulletins.

**Patents End-to-End (PE2E)** is a Master system portfolio consisting of next generation Patent Information Systems. The goal of PE2E is to make the interaction of USPTO's users as simple and efficient as possible in order to accomplish user goals. PE2E is a single web-based examination tool providing users with a unified and robust set of tools. PE2E overhauls the current patents examination baseline through the development of a new system that replaces the existing tools used in the examination process.

**SERCO Patent Processing System (PPS)** is a contractor system that receives information from USPTO so that inventory, identification and classification activities can be performed on patent applications.

**Patent Business Content Management Services (PBCMS)** is a major application that provides file transformation functionality for the USPTO enterprise. As part of the file transformation, the system captures metadata related to the files. This metadata is stored locally within Amazon Web Services (AWS) cloud managed by USPTO Amazon Cloud Services (UACS) and provided to the requesting system/application for processing.

**Patent Business Management Information (PBMI)** is a master system portfolio consisting of a collection of Automated Information Systems (AIS) under the Patents product line. The goal of PBMI is to facilitate and support examiner production, quality assurance, and report dissemination to USPTO employees and contractors. PBMI provides access to easy-to-

acquire validated data and metrics. PBMI will contain the following subsystems: Patents Reporting Oversight (PRO) which has a collection of daily-created denormalized tables that effectively makes reporting more efficient and reliable and Web Marketing and Communications (WMC) which is collection of web services/applications providing business solutions to Patents and/or to the enterprise.

**Trilateral Network (TRINET)** is an Infrastructure information system, and provides secure network connectivity for electronic exchange and dissemination of sensitive patent data between authenticated endpoints at the Trilateral Offices and TRINET members. The Trilateral Offices consist of the USPTO, the European Patent Office (EPO), and the Japanese Patent Office (JPO). The TRINET members consist of the World Intellectual Property Office (WIPO), the Canadian Intellectual Property Office (CIPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO) and the Intellectual Property Office of Australia (IPAU).

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

Once the application is electronically filed, the application is uploaded and then routed through electronic security and formalities review system. Once the application is perfected, an initial classification is automatically determined which is then used to route the application to the proper Technology Center for examination.

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

Patents employees sign in using single sign on. Patent information is extracted from PCAPS-ES and PE2E. Patent examiners log in to the systems and are granted access only to the patent application that has been assigned to them. USPTO System administrators also have access for O&M purposes.

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

The original patent information is submitted directly from the individual from whom the information pertains and is transmitted through various systems. PCAPS-IP receives this information via an interconnection from PE2E and PCAPS-ES or for foreign patents the information is transmitted through TRINET to the foreign patent offices.

*(g) Any information sharing*

Patent examiners are granted access only to the patent application that has been assigned to them. PCAPS-IP sends foreign patents via TRINET to applicable foreign patent offices.

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

5 U.S.C. 301, 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*

This system has been categorized as 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.)*

<b>Changes That Create New Privacy Risks (CTCNPR)</b>					
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.

### **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.)*

<b>Identifying Numbers (IN)</b>					
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 checked="" type="checkbox"/>	i. Credit Card	<input type="checkbox"/>	m. Medical Record	<input type="checkbox"/>
e. File/Case ID	<input checked="" type="checkbox"/>				
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

<b>General Personal Data (GPD)</b>	
------------------------------------	--

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. Marital Status	<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 checked="" type="checkbox"/>	n. Religion	<input type="checkbox"/>		
u. Other general personal data (specify): Nationality.					

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

<b>Distinguishing Features/Biometrics (DFB)</b>					
a. Fingerprints	<input type="checkbox"/>	f. Scars, Marks, Tattoos	<input type="checkbox"/>	k. Signatures	<input type="checkbox"/>
b. Palm Prints	<input type="checkbox"/>	g. Hair Color	<input type="checkbox"/>	l. Vascular Scans	<input type="checkbox"/>
c. Voice/Audio Recording	<input type="checkbox"/>	h. Eye Color	<input type="checkbox"/>	m. DNA Sample or Profile	<input type="checkbox"/>
d. Video Recording	<input type="checkbox"/>	i. Height	<input type="checkbox"/>	n. Retina/Iris Scans	<input type="checkbox"/>
e. Photographs	<input type="checkbox"/>	j. Weight	<input type="checkbox"/>	o. Dental Profile	<input type="checkbox"/>
p. Other distinguishing features/biometrics (specify):					

<b>System Administration/Audit Data (SAAD)</b>					
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"/>	f. Queries Run	<input checked="" type="checkbox"/>	f. Contents of Files	<input type="checkbox"/>
g. Other system administration/audit data (specify):					

<b>Other Information (specify)</b>					

2.2 Indicate sources of the PII/BII in the system. (*Check all that apply.*)

<b>Directly from Individual about Whom the Information Pertains</b>					
---	--	--	--	--	--

In Person	<input type="checkbox"/>	Hard Copy: Mail/Fax	<input type="checkbox"/>	Online	<input type="checkbox"/>
Telephone	<input type="checkbox"/>	Email	<input type="checkbox"/>		
Other (specify):					

<b>Government Sources</b>					
Within the Bureau	<input checked="" 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):					

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

After patent applications submission to PE2E, PCAPS-IP completes quality checks by retrieving data provided by patent applicants from PE2E to minimize errors. Individuals who submit applications are also able to log in to the PE2E and review their application at any time. The individuals may contact USPTO if any of the information is incorrect. The system is secured using appropriate administrative physical and technical safeguards in accordance with the National Institute of Standards and Technology (NIST) security controls (encryption, access control, and auditing). Mandatory IT awareness and role-based training is required for staff who have access to the system and address how to handle, retain, and dispose of data. All access has role-based restrictions and individuals with privileges have undergone vetting and suitability screening. The USPTO maintains an audit trail and performs random, periodic reviews (quarterly) to identify unauthorized access and changes as part of verifying the integrity of administrative account holder data and roles. Inactive accounts will be deactivated and roles will be deleted from the application.

### 2.4 Is the information covered by the Paperwork Reduction Act?

<input checked="" type="checkbox"/>	<p>Yes, the information is covered by the Paperwork Reduction Act.</p> <p>Provide the OMB control number and the agency number for the collection.</p> <p>0651-0031 Patent Processing            0651-0032 Patent Initial Application            0651-0024 Patent Cooperation Treaty (PCT)            0651-0022 Biological Materials            0651-0024 Nucleotide Sequence</p>
-------------------------------------	---

<input type="checkbox"/>	
<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.)*

<b>Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)</b>			
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.)*

<b>Activities</b>			
Audio recordings	<input type="checkbox"/>	Building entry readers	<input type="checkbox"/>
Video surveillance	<input type="checkbox"/>	Electronic purchase transactions	<input type="checkbox"/>
Other (specify):	Click or tap here to enter text.		

<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.)*

<b>Purpose</b>			
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 checked="" 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 the processing of patent applications.

## **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).

Patent applicants provide their name, domicile address, citizenship, phone number, email address work address, work phone number, work email and proprietary business information upon the submission of a patent. Information may also be submitted for patent applications by a patent attorney. If a patent applicant has a patent attorney, the contact information will also be provided.

The information collected is of public, Federal employees and Contractors working on behalf of DOC. Public data is used to file and manage Patent applications. Federal employee and Contractors working on behalf of DOC data is used internally for Patent examiner work, management of Federal employees, and the management of the information technology (IT) systems that support the USPTO.

5.2 Describe any potential threats to privacy, such as insider threat, 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 PCAPS-IP, patent applicants' submissions could be at risk to man-in-the-middle attacks. However; PCAPS-IP requires all user browser communications are secured through the use of Hypertext Transfer Protocol Security / Transport Layer Security (HTTPS/TLS) protocols. Inadvertent private information exposure is a risk and USPTO has policies, procedures, and training to ensure that employees are aware of their responsibility of protecting sensitive information and the negative impact to the agency if there is a loss, misuse, or unauthorized access to or modification of sensitive private information. USPTO requires Annual Security Awareness Training for all employees as well as policies and procedures documented in the Cybersecurity Baseline Policy. All USPTO offices adhere to USPTO Records Management Office's Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citation.

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

<input type="checkbox"/>	The PII/BII in the system will not be shared.
--------------------------	---

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

<input checked="" type="checkbox"/>	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
<input type="checkbox"/>	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
<input type="checkbox"/>	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 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.</p> <p>Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:</p> <p>ICAM-IDaaS SCS PCAPS-ES PE2E PPS PBCMS PBMI TRINET</p> <p>NIST security controls are in place to ensure that information is handled, retained, and disposed of appropriately. For example, advanced encryption is used to secure the data</p>
-------------------------------------	---

	both during transmission and while stored at rest. Access to individual's PII is controlled through the application and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. USPTO requires annual security role based training and annual mandatory security awareness procedure training for all employees. All offices of the USPTO adhere to the USPTO Records Management Office's Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citation.
<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.

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

<b>Class of Users</b>			
General Public	<input 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: <a href="https://www.uspto.gov/privacy-policy">https://www.uspto.gov/privacy-policy</a>
<input checked="" type="checkbox"/>	Yes, notice is provided by other means. Specify how: This PIA provides notice
<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: Patent applicants are required to provide PII and BII in order to apply for a patent. If the PII or BII is not provided the patent cannot be processed. USPTO employees and contractors are required to provide their PII or BII to fulfill their duties at USPTO.

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: The PII and BII requested upon the submission of the patent application is only used for the purpose of processing, granting and publishing the patent. The individual does not have the opportunity to consent to particular uses of their PII/BII.

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: USPTO employees and contractors are able to directly review their PII in PCAPS-IP but need to work with HR or their contracting officer respectively to update it.
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: Patent applicants do not have the right to review or update their PII within PCAPS-IP but would be able to do this through the ingest system (name system).  UPSTO employees and contractors are unable to update their information directly in PCAPS-IP and need to work with HR or their contracting officer respectively.

## **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: PII/BII is monitored, tracked, or recorded via audit logs.
<input checked="" type="checkbox"/>	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 6/13/2025 <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 5 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 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 checked="" type="checkbox"/>	Contracts with customers establish DOC 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).*

PII within the system is secured using appropriate management, operational, and technical safeguards in accordance with NIST requirements. Such management controls include a review process to ensure that management controls are in place and documented in the System Security Privacy Plan (SSPP). The SSPP specifically addresses the management, operational, and technical controls that are in place and planned during the operation of the system. Operational safeguards include restricting access to PII/BII data to a small subset of users. All access has role-based restrictions and individuals with access privileges have undergone vetting and suitability screening. Data is maintained in areas accessible only to authorized personnel. The system maintains an audit trail and the appropriate personnel is alerted when there is suspicious activity. Data is encrypted in transit and at rest.

## Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

- Yes, the PII/BII is searchable by a personal identifier.
- No, the PII/BII is not searchable by a personal identifier.

9.2 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, number, and link. <i>(list all that apply):</i>  <u><a href="#">Patent Application Files--COMMERCE/PAT-TM-7</a></u> <u><a href="#">USPTO PKI Registration and Maintenance System--Commerce/PAT-TM-16</a></u> <u><a href="#">DEPT-25, Access Control and Identity Management System</a></u>
<input type="checkbox"/>	Yes, a SORN has been submitted to the Department for approval on <u><a href="#">(date)</a></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:  <ul style="list-style-type: none"> <li>• Patent Examination Working Files N1-241-10-1:4.2</li> <li>• Patent Examination Feeder Records N1-241-10-1:4.4</li> <li>• Patent Post-Examination Feeder Records N1-241-10-1:4.5</li> </ul>
<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.)*

<b>Disposal</b>			
Shredding	<input type="checkbox"/>	Overwriting	<input type="checkbox"/>
Degaussing	<input type="checkbox"/>	Deleting	<input checked="" type="checkbox"/>
Other (specify): Purging process. When applications are transferred to external agencies, and such applications are determined to be related to national security, such applications are purged from the system.			

## **Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level**

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, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

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

<input checked="" type="checkbox"/>	Identifiability	Provide explanation: The information captured by the PCAPS-IP system such as Employee ID, File ID, Name, Home Address, Telephone Number, Email Address, Work Address, Work Telephone Number, Work Email could identify a particular individual, it could be used to identify a particular individual by itself or when combined with other PII.
<input checked="" type="checkbox"/>	Quantity of PII	Provide explanation: The quantity of PII/BII will be determined by the number of nominations submitted for review. PCAPS-IP processes an estimated 6-7 thousand patents a month.
<input checked="" type="checkbox"/>	Data Field Sensitivity	Provide explanation: Unpublished patent information viewed by the examiners are more sensitive than any other PII/BII viewed in the systems. This data remains sensitive until published. Once published the patent information would become public knowledge.  PCAPS-IP systems are internal to the USPTO employees and examiners can only see patents assigned to their case load.
<input checked="" type="checkbox"/>	Context of Use	Provide explanation: The data captured, stored, or transmitted by the PCAPS-IP system is used to process patent applications.
<input checked="" type="checkbox"/>	Obligation to Protect Confidentiality	Provide explanation: USPTO obligated to protect applicants' identity and application while the application is being processed by USPTO. USPTO must protect the PII of each individual in accordance to the Privacy Act of 1974 undergoing patent prosecution. Based on the data collected USPTO must protect the PII of each individual in accordance to the Privacy Act of 1974.
<input checked="" type="checkbox"/>	Access to and Location of PII	Provide explanation: The information captured, stored, and transmitted by the PCAPS-IP system is maintained within USPTO systems.
<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.)

The PII in this system poses a risk if exposed. System users undergo annual mandatory training regarding appropriate handling of information. Physical access to servers is restricted to only a few authorized individuals. The servers storing the potential PII are located in a highly sensitive zone within the cloud and logical access is segregated with network firewalls and switches through an Access Control list that limits access to only a few approved and authorized accounts. USPTO monitors, in real-time, all activities and events within the servers storing the potential PII data and personnel review audit logs received on a regular bases and alert the appropriate personnel when inappropriate or unusual activity is identified.

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.