

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



**Privacy Impact Assessment
for the
Patent Capture and Application Processing System - Examination
Support (PCAPS-ES)**

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

NICHOLAS CORMIER

Digitally signed by NICHOLAS CORMIER
Date: 2025.09.25 09:49:21 -04'00'

9/25/2025

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 - Examination Support (PCAPS-ES)

Unique Project Identifier: PTOP-005-00

Introduction: System Description

Provide a brief description of the information system.

PCAPS-ES allows the submission, categorization, metadata capture, and Patent Examiner assignment of patent applications within United States Patent and Trademark Office (USPTO).

The purpose of PCAPS-ES is to assign Patents to Patent Examiners for processing, transmitting, storing data, and retrieving images in support of the USPTO's patent application process and its data capture and conversion requirements.

- **Patent Service for Timing and Application Routing (P-STAR)** system determines each examiners proficiency with a given subject matter and uses that data to assign future work to examiners docket.
- **Patent Application Location Monitoring – File Ordering System (PALM FOS)** tracks the physical location and status of issued or abandoned patents, as well as registered or abandoned Trademark files.
- **One Patent Service Gateway (OPSG)** provides security, tracking, logging, error handling, and message queue capabilities, replacing a plethora of legacy services and components
- **Trilateral Document Access (TDA)** provides a service to exchange priority documents with World Intellectual Property Organization (WIPO) member offices (European Patent Office (EPO), Japanese Patent Office (JPO), Korean Intellectual Property Office (KIPO).

Address the following elements:

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

Major Application

(b) System location

Manassas, VA

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

Building, Assets & Property Management (BAPM) - is for federal employees and contractors to help with administrative matters by creating platforms where employees are notified of emergencies, track business-related schedules, and track business continuity for updates as necessary.

Information Delivery Product (IDP) - provide users access to USPTO financial-related documents to support the decision-making activities of managers and analysts. The system provides an interface for users to access the database, generate reports and ability to visualize the data

Information Dissemination Support System (IDSS) - supports the Trademark and Electronic Government Business Division, the Corporate Systems Division (CSD), the Patent Search System Division, the Office of Electronic Information Products, and the Office of Public Information Services. It provides automated support for the timely search and retrieval of electronic text and images concerning patent applications and patents by USPTO internal and external users.

Intellectual Property Leadership Management Support System (IPLMSS) - is a Major Application information system, which provides capabilities and functionality.

Identity Credential Access Management Identity as a Service (ICAM-IDaaS) - is an infrastructure information system that provides authentication and authorization service to secure all USPTO enterprise applications and provides audit ability to user activity.

Enterprise Software Services (ESS) - provides Enterprise Directory Services, Role-Based Access Control System, Email as a Service, USPTO Exchange Services, Symantec Endpoint Protection, Enterprise SharePoint Services, etc.

Enterprise Unix Services (EUS) - is a General Support System with a purpose of providing a LINUX base hosting platform to support other information systems at USPTO. The system supports the underlying operating system (OS), OS patching and updates, and OS level baseline compliance.

Enterprise Desktop Platform (EDP) - is an infrastructure information system that provides a standard enterprise-wide environment that manages desktops and laptops running on the Windows OS, providing United States Government Configuration Baseline (USGCB) compliant workstations.

Enterprise Windows Server (EWS) - is an Infrastructure Information System, and provides a basic hosting platform for major applications that support various USPTO missions. Data is generally owned by the application not the platform.

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)

Network and Security Infrastructure (NSI) - facilitates the communications, secure access, protective services, and network infrastructure support for all USPTO applications.

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 EPO, and the JPO. The TRINET members consist of the WIPO, the Canadian Intellectual Property Office (CIPO), the KIPO, the State Intellectual Property Office of the People's Republic of China (SIPO) and the Intellectual Property Office of Australia (IPAU).

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 Infrastructure Management (SIMS) - provides access to consolidated, block level data storage and files system storage

International Data Exchange-Moderate (IDE) - is a system developed by the USPTO that help exchange published and unpublished application data with international stakeholders, including foreign intellectual property offices (IPOs) and the WIPO.

Patent Business Content Management Services (PBCMS) - Mission of the EventHub system is to provide enterprise service pattern that can be leveraged by USPTO systems for processing documents conversion.

Data Storage Management System (DSMS) - is an infrastructure system that provides archival and storage capabilities securely to the USPTO. The information system is considered an essential component of USPTO's Business Continuity and Disaster Recovery program

Patent Capture and Application Processing System - Capture and Initial Processing (PCAPS-IP) - is a system which provides support to the 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 subsystems that perform specific functions, including submissions, categorization, metadata capture, and patent examiner assignment of patent applications.

Patent End to End (PE2E) - is a Master system portfolio consisting of next generation Patents AIS. 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 will be a single web-based examination tool providing users with a unified and robust set of tools. PE2E will overhaul the current patents examination baseline through the development of a new system that replaces the existing tools used in the examination process. The project stakeholders desire a simple, unified interface that

does not require launching of separate applications in separate windows, and that supports new and improved IT advances.

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.

Patent Search System-Specialized Search (PSS-SS) - this system provides access to specialized data that may include annual submissions of nucleic and amino acid sequence or prior-art searching of polynucleotide and polypeptide sequences, and other types of information that may be more scientific or the technology-based, Patent Linguistic Utility Service (a query by example search system), Chemical Drawing ability, and Foreign Patent Data.

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

PCAPS-ES uses several subsystems to process, transmit, store, and retrieve images to support the data-capture and conversion requirements of the USPTO to support the USPTO patent application process. It allows the submission, categorization, metadata capture, and Patent Examiner assignment of patent applications from internal and external customers of the USPTO.

The purpose of PCAPS-ES is to assign Patents to Patent Examiners for processing, transmitting, storing, and retrieving images in support of the United States Patent and Trademark Office's (USPTO's) patent application process and its data capture and conversion requirements.

- **P-STAR** system determines each examiners proficiency with a given subject matter and uses that data to assign future work to examiners docket.
- **PALM FOS** tracks the physical location and status of issued or abandoned patents, as well as registered or abandoned Trademark files.
- **OPSG** provides security, tracking, logging, error handling, and message queue capabilities, replacing a plethora of legacy services and components
- **TDA** provides a service to exchange priority documents with WIPO member offices EPO, JPO, KIPO.

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

USPTO employees and USPTO contractors, Patent Examiners system administrators, examination support staff, and USPTO network (PTONet) internal users can retrieve the information through a PTONet connection with access granted as-needed and using a least-privileged policy. Retrieval is done via intranet web-interfaces, database interfaces, and network interfaces.

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

Hypertext Transfer Protocol Secure (HTTPS) and Secure Sockets Layer (SSL) are used for all data transmissions to within PTONet.

(g) Any information sharing

PCAPS-ES shares information via its web interface to internal USPTO employees and contractors. Patent applicants PII may be shared with other USPTO systems to communicate directly with patent applicants. TDA shares patent applicant information directly with WIPO and other international patent organizations.

(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,

(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 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.)*

Identifying Numbers (IN)					
a. Social Security*	☐	f. Driver's License	☐	j. Financial Account	☐
b. Taxpayer ID	☐	g. Passport	☐	k. Financial Transaction	☐
c. Employer ID	☐	h. Alien Registration	☐	l. Vehicle Identifier	☐
d. Employee ID	☒	i. Credit Card	☐	m. Medical Record	☐
e. File/Case ID	☒				
n. Other identifying numbers (specify): Patent Application number, Patron ID					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	☒	h. Date of Birth	☐	o. Financial Information	☐
b. Maiden Name	☐	i. Place of Birth	☒	p. Medical Information	☐
c. Alias	☐	j. Home Address	☒	q. Military Service	☐
d. Gender	☐	k. Telephone Number	☒	r. Criminal Record	☐
e. Age	☐	l. Email Address	☒	s. Marital Status	☐
f. Race/Ethnicity	☐	m. Education	☐	t. Mother's Maiden Name	☐
g. Citizenship	☒	n. Religion	☐		
u. Other general personal data (specify): Country Code, Inventor name					

Work-Related Data (WRD)					
a. Occupation	☐	e. Work Email Address	☒	i. Business Associates	☐
b. Job Title	☐	f. Salary	☐	j. Proprietary or Business Information	☒
c. Work Address	☒	g. Work History	☐	k. Procurement/contracting records	☐
d. Work Telephone Number	☒	h. Employment Performance Ratings or	☐		

		other Performance Information			
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	☐	f. Scars, Marks, Tattoos	☐	k. Signatures	☐
b. Palm Prints	☐	g. Hair Color	☐	l. Vascular Scans	☐
c. Voice/Audio Recording	☐	h. Eye Color	☐	m. DNA Sample or Profile	☐
d. Video Recording	☐	i. Height	☐	n. Retina/Iris Scans	☐
e. Photographs	☐	j. Weight	☐	o. Dental Profile	☐
p. 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	☒	f. 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 Describe how the accuracy of the information in the system is ensured.

PCAPS-ES employs system checks to ensure accuracy, completeness, validity, and authenticity. Each PCAPS-ES component has established specific rules or conditions for checking the syntax of information input to the system such as numbers or text; numerical ranges and acceptable values are utilized to verify that inputs match specified definitions for format and content. PCAPS-ES components have rules in place to validate the content of input information based on field requirements (i.e., date fields are validated for date format and legitimacy). Some PCAPS-ES applications have rules in place to validate the content of input information based on field requirements (i.e., date fields are validated for date format and legitimacy).

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. 0651-0031 Patent Processing 0651-0032 Initial Patent Processing 0651-0033 Post Allowance and Refilling 0651-0035 Representative and Address Provisions 0651-0071 Matters Related to First Inventor to File
☐	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 (TUCPBNDP)			
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 Activities3.1 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): Click or tap here to enter text.			

☒	There are not any IT system supported activities which raise privacy risks/concerns.
-------------------------------------	--

Section 4: Purpose of the System

- 4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated.
(Check all that apply.)

Purpose			
For a Computer Matching Program	☐	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 following PII/BII collected is of the public (U.S. and foreign) Federal employees and DOC contractors. Employee ID, File/Case ID, Name, Citizenship, Place of Birth, Home Address, Telephone Number, Email Address, Country Code, Work Address, Work Telephone Number, Work Email Address, Propriety or Business Information. Public data is used to file and manage Patent applications. Federal employee data is used for Patent examiner work, management of Federal employees and contractors, and the management of the 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.)

In the event of computer failure, insider threats, or attack against the system by adversarial or foreign entities, any potential PII data stored within the system could be exposed. To avoid a breach, the system has certain security controls in place to ensure the information is handled, retained, and disposed of appropriately. 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. These audit trails are based on application server out-of-the-box logging reports reviewed by the Information System Security Officer (ISSO) and System Auditor and any suspicious indicators such as browsing will be immediately investigated and appropriate action taken. Also, system users undergo annual mandatory training regarding appropriate handling of information.

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 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 adhere to the USPTO Records Management Office's Comprehensive Records Schedule or the General Records Schedule and the corresponding disposition authorities or citations.

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

☐	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
☒	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
☐	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.

☒	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: DSMS EWS EDP EUS ESS NSI ICAM-IDaaS IDSS IPLMSS IDE-M FPNG PE2E PBCMS PCAPS-IP PBMI PSS-SS SCS SIMS TRINET 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 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 adhere to the
-------------------------------------	--

	USPTO Records Management Office's Comprehensive Records Schedule or the General Records Schedule and the corresponding disposition authorities or citations.
☐	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.*)

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 policy. The privacy policy can be found at: https://www.uspto.gov/privacy-policy	
☒	Yes, notice is provided by other means.	Specify how: This PIA provides notice
☐	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: 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 do not

		have an opportunity to decline to provide PII/BII within PCAPS-ES as it is necessary for the security of the system and the work the individual needs to do within PCAPS-ES.
--	--	--

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

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: USPTO employees and contractors are able to directly review their PII in PCAPS-ES but are unable to directly.
☒	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-ES but would be able to do this through the ingest system. UPSTO employees and contractors are unable to update their information directly in PCAPS-ES 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.)*

☐	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: PII/BII is monitored, tracked, or recorded via audit logs.
☒	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): 5/25/2025 ☐ 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 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).
☒	A security assessment report has been reviewed for the 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 DOC 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).*

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."

☒	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> PAT-TM-7 Patent Application Files PAT-TM-16 USPTO PKI Registration and Maintenance System DEPT-25 Access Control and Identity Management System
☐	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: · 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
☐	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 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.)

☐	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 level.
(Check all that apply.)

☒	Identifiability	Provide explanation: The information captured by the PCAPS-ES system such as Employee ID, File ID, Name, Home Address, Telephone Number, Email Address, Work Address, Work Telephone Number Citizenship, Work Email could identify a particular individual, it could be used to identify a particular individual by itself or when combined with other PII
☒	Quantity of PII	Provide explanation: The quantity of PII/BII will be determined by the number of nominations submitted for review. PCAPS-ES processes an estimated 6-7 thousand patents a month.
☒	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-ES systems are internal to the USPTO employees and examiners can only see patents assigned to their case load.
☒	Context of Use	Provide explanation: The data captured, stored, or transmitted by the PCAPS-ES system is used to process patent applications.
☒	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.
☒	Access to and Location of PII	Provide explanation: The information captured, stored, and transmitted by the PCAPS-ES system is maintained within USPTO systems.
☐	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.

☐	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.