Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
Patent Administrative Center (PAC)

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

CHARLES CUTSHALL Digitally signed by CHARLES CUTSHALL
Date: 2025.05.06 11:51:29 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO Patent Administrative Center (PAC)

Unique Project Identifier: PPL-PAC-01-00

<u>Introduction</u>: System Description

Provide a brief description of the information system.

Patent Administrative Center (PAC) is a United States Patent and Trademark Office (USPTO) developed, cloud-based software application that is used for pre-review of patent process for routing and security reviews of patent applications.

PAC is comprised of Patent Application Services and Security (PASS) and Patents Service for Timing and Application Routing (P-STAR). PASS supports the entire security review process and has access to the patent applications. P-STAR determines each examiners proficiency with a given subject matter and uses that data to assign future work to examiners docket.
Address the following elements:

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

Major Application

(b) System location

The physical location of the servers which house or process the information is located in USPTO Amazon Web Services (AWS) US East/West, in Virginia.

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

USPTO Amazon Cloud Services (UACS): The UACS Infrastructure-as-a-Service (IaaS) platform used to support USPTO Application Information Systems (AIS) hosted in the AWS East/West environment. UACS leverages AWS IaaS mode that enables on-demand Internet access to a shared pool of configurable computing resources including servers, storage, network infrastructure, and other web-based services.

Database Services (DBS) is an Infrastructure information system, and provides a Database Infrastructure to support 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.

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 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.

Patent Search System – Specialized Search and Retrieval (PSS-SS): The PSS-SS is a Master system that supports the Patent Cost Center. It is considered a mission critical system. PSS-SS provides access to highly specialized data that may include annual submissions of nucleic and amino acid sequence or prior-art searching of polynucleotide and polypeptide sequences.

Security and Compliance Services (SCS): 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.

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

(d) **Identity as a Service (ICAM IDaaS):** Provides user authentication for PAC

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

PASS

Once the application is electronically filed, the application is uploaded and then routed through electronic security review system. Once the application is cleared, an initial classification is automatically determined, which is then used to route the application to the proper Technology Center for examination. If the application fails the initial review, the patent is referred to the next level for review until the patent is eventually referred to external agency for security order.

P-STAR

By using Cooperative Patent Classification (CPC) and historical Patent Application Locating and Monitoring (PALM) data, the P-STAR system determines each examiner's proficiency with a given subject matter and attempt to use that to assign future work. Patent Examiners will log into the P-STAR system to view what subject areas they are qualified to work with via their portfolio. Administrators or Managers can log into P-STAR to view Patent Examiners portfolio and also to manually add subject areas to portfolios. Patent Examiners can only view subject areas assigned to their portfolio to review for accuracy.

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

USPTO patent examiners use their Government Furnished Equipment (GFE) to log-in to PAC using OKTA Identity as a Service (IDaaS) for authentication, and can review and track patent applications through the patent lifecycle.

Individuals 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. Patents can be searched through various methods.

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

Information is transmitted between the PAC system and the Patent Examiners of the system via Hypertext Transfer Protocol Secure (HTTPS) protocol and Hypertext Transfer Protocol (HTTP) Transport Layer Security (TLS) encryption using certificates.

(h) The original patent information is submitted directly by the individual from whom the information pertains and is transmitted through various systems to PAC. PAC receives domestic and foreign patent information via an interconnection from Patent End to End (PE2E) and Patent Business Content Management Services (PBCMS).

(i) *Any information sharing*

P-STAR: Patent applications routed through the timing and routing service are assessed for examiner proficiency. Once P-STAR creates the docketing and timing recommendations to assign future work to examiners docket, it sends the examiner application pairs for potential docket to Docket Application Viewer (DAV) for implementation. PSTAR also sends preliminary timing recommendation, learning curve and transition time hours which are number of hours an examiner can use to complete the work for the given application to DAV.

PASS: Patents that do not pass the initial security review are routed through electronic security review system. Once the application is cleared, an initial classification is automatically determined, which is then used to route the application to the proper Technology Center for examination. If the application fails the initial review, the patent is referred to the next level for review until the patent is eventually referred to external agency for security order.

(j) *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, 2, 6, 42(c), 115, 184, 261

(k) *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.)*

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 numbers					
*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):					

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.

The information for the Patents is provided from the individual submitting the patent or their representative. 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?

☒	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 Applications
☐	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 (TUCPBNPD)			
Smart Cards	☐	Biometrics	☐
Caller-ID	☐	Personal Identity Verification (PIV) Cards	☐
Other (specify):			

☒	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

<u>Section 3</u>: 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): 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).

Patent applicants provide their name, citizenship, domicile address, 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 and contractor 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 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.)

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 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.

<u>Section 6</u>: 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): Patent Application owners	☒	□	□

□	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 infomation 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: ICAM-IDaaS Serco PPS SCS PSS-SS PE2E PCAPS-ES UACS 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 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.
□	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 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: 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.

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 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.

☒	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 PAC but are unable to directly update their PII in the system.
☒	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 PAC but would be able to do this through the ingest system Central Enterprise Data Repository (CEDR). UPSTO employees and contractors are unable to update their information directly in PAC 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: 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): ☒ 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 information system and it has been detemined 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 te 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. *(list all that apply)*: COMMERCE/PAT-TM-7, Patent Application Files COMMERCE/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 (date).
□	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.)*

General Records Schedules (GRS) | National Archives

☒	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 • Information technology operations and maintenance records. GRS 3.1.020 (includes audit, security, system logs) • P-STAR is an unscheduled system. (Review and approval of records schedule is pending by NARA)
□	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- IP 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. PAC 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. PAC 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 PAC 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. UPSTO 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 PAC 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.