Template Version Number: 01-2021

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: 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

Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry
Date: 2022.03.14 09:28:30 -04'00'

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.

PCAPS-IP is a Major Application that which provides support to 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 information systems that perform specific functions, including submissions, categorization, metadata capture, and patent examiner assignment of patent applications. PCAPS-IP users include both internal USPTO personnel as well as the public.

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 at USPTO, 600 Dulany Street, 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:

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 United States Patent and Trademark Office (USPTO) IT applications.

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

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.

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

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.

World Intellectual Property Organization (WIPO): The World Intellectual Property Organization or WIPO is a UN specialized agency created in 1967 to promote intellectual property (IP) protection and encourage creative activity all over the world. WIPO is basically a global forum for IP policy, services, information and cooperation.

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

EFS-Web facilitates online patent application submissions for patent examiners to administratively process towards grant/no grant decision. Web surveys are conducted semi-

annually to solicit input from customers of their perception of examination quality. Checker application allows the public to check sequence listings before submission to the USPTO.

The PALM Pre-Exam system supports the prosecution and related administrative functions of a patent application through its life cycle; and also tracks, monitors, and reports on the prosecution status of patent applications. PALM Pre-Exam supports the processing of over 350,000 applications each year.

The PRS produces many productivity and statistical reports that are crucial to the Patents Corps business operation. The PRS processes and delivers reports to Patents Corp, supporting various PALM subsystems and business areas, including: PALM-EXPO, Pre-Exam, File Ordering System (FOS), Infrastructure, and PCT OPS. These reports are available via the USPTO Intranet on-line and on-demand to over 5,000 Examiners, Directors, Supervisory Patent Examiners (SPEs), and Clerical staff.

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

(f) How information is transmitted to and from the system
All PCAPS-IP communications must traverse the USPTO's Network and Security System which facilitates the communications, secure access, protective services, and network infrastructure support for all USPTO applications.

(g) Any information sharing
PCAPS-IP applications facilitate patent examiners to collaborate internally and with their Intellectual Property international partners.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information
35 U.S.C. 1, 35 U.S.C. 2, 35 U.S.C. 115, 35 U.S.C. 184, 35 U.S.C. 261

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system
PCAPS-IP has a FIPS 199 categorization level of 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):					
*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.

PCAPS-IP does not perform Personally Identifiable Information (PII) verification as it is the patent applicant's responsibility to ensure accurate contact information to facilitate correspondence between the applicant and the USPTO examiners. However; Business Identifiable Information (BII) information is verified through the patent process. Access controls, including the concept of least privilege, are in place within the system to protect the integrity of this data as it is processed or stored.

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. The data processed by this system is collected under the following OMB control numbers: 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 (TUCPBNPD)			
Smart Cards	☐	Biometrics	☐
Caller-ID	☐	Personal Identity Verification (PIV) Cards	☐
Other (specify):			

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

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings	☐	Building entry readers	☐
Video surveillance	☐	Electronic purchase transactions	☐
Other (specify):			

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

Section 4: Purpose of the System

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

Purpose			
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 information collected is of the public (U.S. and foreign) and Federal employees. Public data is used to file and manage Patent applications. Federal employee data is used internally for Patent examiner work, management of Federal employees, and the management of the 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 EFS-Web, patent applicants submissions could be at risk to man-in-the-middle attacks. However; EFS-Web requires all user browser communications are secured through the use of 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.

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: USPTO's Patent Search System Primary Search (PSS-PS); Patent Capture and Application Processing System– Examination Support (PCAPS-ES); Security and Compliance Services (SCS); Patent End to End (PE2E); Patent Search System– Specialized Search and Retrieval (PSS-SS) and Serco Patent Processing System (PPS). • Information is protected through a layered security approach which incorporates the use of secure authentication, access control, mandatory configuration settings, firewalls, Virtual Private Network (VPN), and encryption, where required. Internally within USPTO, data transmission confidentiality controls are provided by PTOnet. Serco PPS assists USPTO in processing of Patent Applications, by providing the services which: (1) Pre-classify patent applications according to USPTO classification schedules; (2) Route applications through the classification process; (3) Provide a support application that will guide a patent classifier through the classification process. World Intellectual Property Organization (WIPO) / Foreign Patent Offices: For external data transfer to WIPO, data is transmitted across USPTO's Trilateral which is a Point-to-Point dedicated Virtual Private Network (VPN).
☐	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 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:
☐	No, notice is not provided.	Specify why not:

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

☒	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Patent applicants are advised that information submitted to USPTO is voluntary. Individuals grant consent by filing out a patent registration and submitting it for processing. They are notified that the information that they submit will become public information. They may decline to provide PII by not submitting ab application.
☐	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

☒	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: A patent applicant's submission constitutes their consent to the use of the information for the purpose(s) stated at the time of collection.
☐	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

☒	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: During patent submission via EFS-Web, applicants have opportunities to update PII/BII data prior to final submission. After a patent submission, users must contact the Electronic Business Center for PII updates. All subsequent BII updates occur within PCAPS-ES system.
☐	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

☐	All users signed a confidentiality agreement or non-disclosure agreement.
☐	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
☒	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
☒	Access to the PII/BII is restricted to authorized personnel only.
☒	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: 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): _6/17/2022_____ ☐ 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 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).*

PCAPS-IP collects voluntary applicant(s) correspondence information to facilitate direct communications between the applicant(s) and the Office. PCAPS-IP applications are managed and secured by the USPTO's Active Directory (AD) and Unix Enterprise infrastructure and other Office of the Chief Information Officer (OCIO) established technical controls, which include password authentication at the server and database levels. Hypertext Transfer Protocol Security HTTPS) is used for all data transmissions to and from the Internet, USPTO Demilitarized Zone (DMZ), and PTOnet. A dedicated socket is used to perform encryption and decryption.

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)*: Patent Application Files--COMMERCE/PAT-TM-7 USPTO PKI Registration and Maintenance System--Commerce/PAT–TM–16
☐	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.)*

☒	There is an approved record control schedule. Provide the name of the record control schedule: • Evidentiary Patent Applications N1-241-10-1:4.1 • Patent Examination Working Files N1-241-10-1:4.2 • Patent Examination Feeder Records N1-241-10-1:4.4 • Patent Post-Examination Feeder Records N1-241-10-1:4.5 • Patent Case Files, Granted N1-241-10-1:2 *Abandoned Patent Applications, Not Referenced in Granted Case File N1-241-10-1:3
☐	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
☒	Yes, retention is monitored for compliance to the schedule.
☐	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	☒	Overwriting	☐
Degaussing	☐	Deleting	☒
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact 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 etc. could identify a particular individual.
☒	Quantity of PII	Provide explanation: The quantity of PII/BII will be determined by the number of nominations submitted for review.
☒	Data Field Sensitivity	Provide explanation: PII stored in the system is data collected from USTPO employees and contractor personnel in which the information is confidential and unique to those individuals. Any unauthorized access, modification, and/or disclosure of sensitive data would have a Moderate impact on the organization and its operations.
☒	Context of Use	Provide explanation: The data captured, stored, or transmitted by the PCAPS-IP system is used to process patent applications.
☒	Obligation to Protect Confidentiality	Provide explanation: USPTO examiners are obligated to protect applicants' identity and application while the application is 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-IP system is maintained within USPTO systems. No sensitive-PII is shared external to PCAPS-IP system.

☐	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

The threats to the system are insider threats and foreign entities. The information in the system can be retrieved by the public. USPTO implements security and management controls to prevent the inappropriate disclosure of sensitive information. Security controls are employed to ensure information is resistant to tampering, remains confidential as necessary, and is available as intended by the Agency and as expected by authorized users. Management controls are utilized to prevent the inappropriate disclosure of sensitive information. NSI and SCS provide additional automated transmission and monitoring mechanisms to ensure that PII/BII information is protected and not breached by external entities.

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.

Points of Contact and Signatures

System Owner
Name: Huong Esposo
Office: Office of Patent Information Management (OPIM)
Phone: (571) 272-5685
Email: Huong.Esposo@uspto.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: Users, Esposo, Huong Digitally signed by Users, Esposo, Huong Date: 2022.03.08 12:55:16 -05'00'

Date signed: _____

Chief Information Security Officer
Name: Don Watson
Office: Office of the Chief Information Officer (OCIO)
Phone: (571) 272-8130
Email: Don.Watson@uspto.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: Users, Watson, Don Digitally signed by Users, Watson, Don Date: 2022.03.08 15:07:59 -05'00'

Date signed: _____

Privacy Act Officer
Name: Ezequiel Berdichevsky
Office: Office of General Law (O/GL)
Phone: (571) 270-1557
Email: Ezequiel.Berdichevsky@uspto.gov

I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA.

Signature: Users, Berdichevsky, Ezequiel Digitally signed by Users, Berdichevsky, Ezequiel Date: 2022.03.07 09:50:10 -05'00'

Date signed: _____

Bureau Chief Privacy Officer and Co-Authorizing Official

Name: Henry J. Holcombe
Office: Office of the Chief Information Officer (OCIO)
Phone: (571) 272-9400
Email: Jamie.Holcombe@uspto.gov

I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.

Signature: Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry Date: 2022.03.08 16:06:50 -05'00'

Date signed: _____

Co-Authorizing Official
Name: Andrew Faile
Office: Office of the Commissioner for Patents
Phone: (571) 272-8800
Email: Andrew.Faile@uspto.gov

I certify that this PIA accurately reflects the representations made to me herein by the System Owner, the Chief Information Security Officer, and the Chief Privacy Officer regarding security controls in place to protect PII/BII in this PIA.

Signature: Users, Faile, Andrew Digitally signed by Users, Faile, Andrew Date: 2022.03.09 19:09:03 -05'00'

Date signed: _____

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.