Version Number: 01-2017

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

Privacy Impact Assessment
for the
Cardinal IP (CIP) Patent Cooperation Treaty Search Recordation System (PCTSRS)

Reviewed by: David Chiles, 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

CATRINA PURVIS

Digitally signed by CATRINA PURVIS
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=CATRINA PURVIS, 0.9.2342.19200300.100.1.1=13001002875743
Date: 2018.06.15 18:20:04 -04'00'

June 15, 2018

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO Cardinal IP (CIP) Patent Cooperation Treaty Search Recordation System (PCTSRS)

Unique Project Identifier: [1860] PTOC-018-00

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

(a) a general description of the information in the system

The Cardinal IP (CIP) Patent Cooperation Treaty Search Recordation System (PCTSRS) is a system that performs Patent Cooperation Treaty (PCT) searches and written opinions on behalf of the United States Patent and Trademark Office (USPTO). PCTSRS provides authenticated employees access to Patent Cooperation Treaty (PCT) applications. The purpose of this system is to support the USPTO's international application or PCT application process. The PCT provides a unified procedure for filing patent applications to protect inventions in each of its Contracting States. PCTSRS facilitates PCT searches and enables CIP employees to submit an accompanying written opinion regarding the patentability of the invention in question.

PCTSRS is an external contractor system with production servers located at a remote Tier III data center in Oak Brook, IL. The CIP data center facility includes physical security implementations including proximity card access controls, hand-geometry biometric locks, video surveillance, and building security. The PCTSRS system consists of several servers for web, email, database, backup, and directory services, as well as local workstations located at CIP's corporate offices, that store, process, and/or transmit USPTO data in the form of Patent Cooperation Treaty applications. PCT application documents are transferred to CIP directly from USPTO via a secure connection.

PCTSRS is only accessible by authenticated employees from within the CIP network. There is no public access to the PCTSRS system. PCT opinions are submitted from CIP directly to the USPTO via a secure connection.

(b) a description of a typical transaction conducted on the system

PCT application documents are transferred to CIP directly from USPTO via a secure connection. A CIP employee is assigned a PCT application to search based on their area of expertise. The CIP employee performs the PCT search and submits an accompanying written opinion regarding the patentability of the invention in question. The PCT opinions are submitted from CIP directly to the USPTO via a secure connection.

(c) any information sharing conducted by the system
All PCT applications and PCT opinions are shared only between CIP and USPTO via a secure connection.

(d) a citation of the legal authority to collect PII and/or BII

35 U.S.C. 1, 2, 115, and 261; E.O. 9424; 5 U.S.C. 301;

(e) the Federal Information Processing Standard (FIPS) 199 security impact category for the system is ***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.)*

☒ This is an existing information system in which changes do not create new privacy risks. *Continue to answer questions, and complete certification.*

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):					

Section 2: Information in the System

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

Identifying Numbers (IN)					
a. Social Security*	☐	e. File/Case ID	☒	i. Credit Card	☐
b. Taxpayer ID	☐	f. Driver's License	☐	j. Financial Account	☐
c. Employer ID	☐	g. Passport	☐	k. Financial Transaction	☐
d. Employee ID	☐	h. Alien Registration	☐	l. Vehicle Identifier	☐
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					
*If SSNs are collected, stored, or processed by the system, please explain if there is a way to avoid such collection in the future and how this could be accomplished:					

General Personal Data (GPD)					
a. Name	☒	g. Date of Birth	☐	m. Religion	☐
b. Maiden Name	☐	h. Place of Birth	☐	n. Financial Information	☐
c. Alias	☐	i. Home Address	☒	o. Medical Information	☐
d. Gender	☐	j. Telephone Number	☒	p. Military Service	☐
e. Age	☐	k. Email Address	☒	q. Physical Characteristics	☐
f. Race/Ethnicity	☐	l. Education	☐	r. Mother's Maiden Name	☐

s. Other general personal data (specify): Citizenship

Work-Related Data (WRD)					
a. Occupation	☒	d. Telephone Number	☒	g. Salary	☐
b. Job Title	☒	e. Email Address	☒	h. Work History	☐
c. Work Address	☒	f. Business Associates	☐		
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	☐	d. Photographs	☐	g. DNA Profiles	☐
b. Palm Prints	☐	e. Scars, Marks, Tattoos	☐	h. Retina/Iris Scans	☐
c. Voice Recording/Signatures	☐	f. Vascular Scan	☐	i. Dental Profile	☐
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	☐	c. Date/Time of Access	☐	e. ID Files Accessed	☐
b. IP Address	☐	d. Queries Run	☐	f. Contents of Files	☐
g. Other system administration/audit data (specify):					

Other Information (specify)

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

Directly from Individual about Whom the Information Pertains					
In Person	☐	Hard Copy: Mail/Fax	☐	Online	☐
Telephone	☐	Email	☐		
Other (specify):					

Government Sources					
Within the Bureau	☒	Other DOC Bureaus	☐	Other Federal Agencies	☐
State, Local, Tribal	☐	Foreign	☐		
Other (specify):					

Non-government Sources					
Public Organizations	☐	Private Sector	☐	Commercial Data Brokers	☐
Third Party Website or Application			☐		
Other (specify):					

2.3 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			
To determine eligibility	☐	For administering human resources programs	☐
For administrative matters	☒	To promote information sharing initiatives	☐
For litigation	☐	For criminal law enforcement activities	☐
For civil enforcement activities	☐	For intelligence activities	☐
To improve Federal services online	☐	For employee or customer satisfaction	☐
For web measurement and customization technologies (single-session)	☐	For web measurement and customization technologies (multi-session)	☐
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The PII/BII that is collected is used to identify PCT patent applicants. The information is collected and disseminated by the Patent ingress systems owned and operated by USPTO. The PCTSRS system does not disseminate this information outside of the organization.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	☐	☒	☐
DOC bureaus	☐	☐	☐
Federal agencies	☐	☐	☐
State, local, tribal gov't agencies	☐	☐	☐
Public	☐	☐	☐
Private sector	☐	☒	☐
Foreign governments	☐	☐	☐
Foreign entities	☐	☐	☐
Other (specify):	☐	☐	☐

☐	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

☒	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: PCTSRS connects to the USPTO File Transfer system which is a part of the NSI Master System. In accordance with the USPTO Privacy Policy guidelines, the Cardinal IP (CIP) PCTSRS system is designed and administered to ensure the confidentiality of PII provided to PCTSRS by USPTO. Bibliographic data (Inventor name, Inventor address, Citizenship, Correspondence address, Employer name and address, Telephone number[s], and E-mail address) are collected from the applicant or applicant's legal representative and attached to the electronic patent application files sent to PCTSRS. During processing, the information is passed through to various stages of the PCTSRS workflow. The information is not shared with any entity outside of PCTSRS operational facility. Specific safeguards that are employed by Cardinal IP to protect the patent applications include: • The PCTSRS system and its facility are physically secured and closely monitored. Only individuals authorized by PCTSRS to access USPTO data are granted logical access to the system. • All patent information is encrypted when transferred between PCTSRS and USPTO using secure electronic methods. • Technical, operational, and management security controls are in place at Cardinal IP and are verified regularly. • Periodic security testing is conducted on the PCTSRS system to help assure than any new security vulnerabilities are discovered and fixed. • All Cardinal IP personnel are trained to securely handle patent information and to understand their responsibilities for protecting patents.
☐	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

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

Class of Users			
General Public	☐	Government Employees	☐
Contractors	☒		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

☒	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.
☐	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: _____.

☒	Yes, notice is provided by other means.	Specify how: Notice is provided at the time of collection by the patent front-end systems.
☐	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: Individuals may have the opportunity to decline to provide their PII/BII. That option would be offered by the primary patent application ingress system, which is covered under the system of records at USPTO: COMMERCE/PAT-TM-1, Attorneys and Agents Registered or Recognized to Practice Before the Office; COMMERCE/PAT-TM-7, Patent Application Files; COMMERCE/PAT-TM-9, Patent Assignment Records; & COMMERCE/PAT-TM-10, Deposit Accounts and Electronic Funds Transfer Profiles. That information is volunteered by individuals as a part of the patent application process.

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: Individuals may have the opportunity to consent to particular uses of their PII/BII. That option would be offered by the primary patent application ingress system, which is covered under the system of records at USPTO: COMMERCE/PAT-TM-1, Attorneys and Agents Registered or Recognized to Practice Before the Office; COMMERCE/PAT-TM-7, Patent Application Files; COMMERCE/PAT-TM-9, Patent Assignment Records; & COMMERCE/PAT-TM-10, Deposit Accounts and Electronic Funds Transfer Profiles. That information is volunteered by individuals as a part of the patent application process.

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:
☒	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: Individuals may have the opportunity to review/update the PII/BII pertaining to them. That option would be offered by the primary patent application ingress system, which is covered under the system of records at USPTO: COMMERCE/PAT-TM-1, Attorneys and Agents

		Registered or Recognized to Practice Before the Office; COMMERCE/PAT-TM-7, Patent Application Files; COMMERCE/PAT-TM-9, Patent Assignment Records; & COMMERCE/PAT-TM-10, Deposit Accounts and Electronic Funds Transfer Profiles.

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:
☒	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): ___05/16/2018_____ ☐ 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 (POAM).
☒	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
☒	Contracts with customers establish ownership rights over data including PII/BII.
☒	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
☐	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

PCTSRS is an internal web docketing system that is only accessible by authenticated/authorized CIP employees. This system is not publically accessible via the Internet. PCTSRS production servers are located at a remote Tier III data center. This data center facility includes physical security implementations including proximity card access controls, hand-geometry biometric locks, video surveillance, and building security. PCT data is only accessible by properly screened CIP employees who require this data to perform their job. The PCTSRS system logs access to PCT data. All data transfers between the USPTO and CIP are performed over encrypted connections.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

☒	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: PAT/TM—1 Attorneys and Agents Registered or Recognized to Practice Before the Office PAT/TM—7 Patent Application Files PAT/TM—9 Patent Assignment Records PAT/TM—10 Deposit Accounts and Electronic Funds Transfer Profiles
☐	Yes, a SORN has been submitted to the Department for approval on (date).
☐	No, a SORN is not being created.

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)
☐	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
☒	Yes, retention is monitored for compliance to the schedule.
☐	No, retention is not monitored for compliance to the schedule. Provide explanation:

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

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

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

☐	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
☒	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
☐	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

☒	Identifiability	Provide explanation: Occupation, name, title, address, phone number, & email address.
☐	Quantity of PII	Provide explanation:
☐	Data Field Sensitivity	Provide explanation:
☒	Context of Use	Provide explanation: Information is used to facilitate PCT searches by contractors working outside of the USPTO environment.
☐	Obligation to Protect Confidentiality	Provide explanation:
☒	Access to and Location of PII	Provide explanation: Because the information containing PII must be transmitted outside of the USPTO environment, there is an added need to ensure the confidentiality of information during transmission.
☐	Other:	Provide explanation:

Section 12: Analysis

12.1 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.

12.2 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.