

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



**Privacy Impact Assessment
for the
Cardinal Intellectual Property (CIP) Patent Cooperation Treaty
Search Recordation System (PCTSRs)**

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: 2025.02.27 14:25:02 -05'00'

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

Date

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

Unique Project Identifier: PTOC-018-00

Introduction: System Description

Provide a brief description of the information system.

The Cardinal Intellectual Property (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 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 production servers are located at a remote Tier III data center. 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 CIP 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. The CIP network is protected by firewalls, anti-virus, and anti-spam systems. The CIP data center facility includes physical security implementations including proximity card access controls, hand-geometry biometric locks, video surveillance, and building security.

Address the following elements:

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

PCTSRS is a general support system.

(b) System location

PCTSRS production servers are located at a remote Tier III data center in Oakbrook, IL.

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

PCTSRS interconnects with:

Network and Security Infrastructure System (NSI): The 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 the USPTO IT applications.

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

The PCTSRS system consists of several servers for web, database, backup, and directory services, as well as local workstations located at CIP's corporate offices in Evanston, IL. PCTSRS facilitates PCT searches and enables CIP employees to submit an accompanying written opinion regarding the patentability of the invention in question. PCT application documents and patentability opinions are transferred between CIP and USPTO via a secure file transfer system hosted and maintained by the USPTO.

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

Users retrieve data from the system via an internal web application (not Internet facing) which is secured by Transport Layer Security (TLS) protocol.

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

Data is transmitted between PCTSRS and USPTO uses an end-to-end secure file transfer solution.

(g) Any information sharing

Information sharing is between PCTSRS and the USPTO. This information is shared within the bureau and with authorized contractors from within the CIP network.

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

35 U.S.C. 1, 2, 41, 115, 261, and 351-376; E.O. 9424; 5 U.S.C. 301

(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 | <input type="checkbox"/> | d. Significant Merging | <input type="checkbox"/> | g. New Interagency Uses | <input type="checkbox"/> |
| b. Anonymous to Non-Anonymous | <input type="checkbox"/> | e. New Public Access | <input type="checkbox"/> | h. Internal Flow or Collection | <input type="checkbox"/> |
| c. Significant System Management Changes | <input type="checkbox"/> | f. Commercial Sources | <input type="checkbox"/> | i. Alteration in Character of Data | <input type="checkbox"/> |
| j. Other changes that create new privacy risks (specify): | | | | | |

☐ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

☒ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

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

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

| | | | | | |
|---|-------------------------------------|---------------------|-------------------------------------|--------------------------|--------------------------|
| General Personal Data (GPD) | | | | | |
| a. Name | <input checked="" type="checkbox"/> | h. Date of Birth | <input type="checkbox"/> | o. Financial Information | <input type="checkbox"/> |
| b. Maiden Name | <input type="checkbox"/> | i. Place of Birth | <input type="checkbox"/> | p. Medical Information | <input type="checkbox"/> |
| c. Alias | <input type="checkbox"/> | j. Home Address | <input checked="" type="checkbox"/> | q. Military Service | <input type="checkbox"/> |
| d. Gender | <input type="checkbox"/> | k. Telephone Number | <input checked="" type="checkbox"/> | r. Criminal Record | <input type="checkbox"/> |
| e. Age | <input type="checkbox"/> | l. Email Address | <input checked="" type="checkbox"/> | s. Marital Status | <input type="checkbox"/> |
| f. Race/Ethnicity | <input type="checkbox"/> | m. Education | <input type="checkbox"/> | t. Mother's Maiden Name | <input type="checkbox"/> |
| g. Citizenship | <input checked="" type="checkbox"/> | n. Religion | <input type="checkbox"/> | | |
| u. Other general personal data (specify): | | | | | |

| |
|--------------------------------|
| Work-Related Data (WRD) |
|--------------------------------|

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

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

| | | | | | |
|--|-------------------------------------|------------------------|-------------------------------------|----------------------|--------------------------|
| System Administration/Audit Data (SAAD) | | | | | |
| a. User ID | <input checked="" type="checkbox"/> | c. Date/Time of Access | <input checked="" type="checkbox"/> | e. ID Files Accessed | <input type="checkbox"/> |
| b. IP Address | <input checked="" type="checkbox"/> | f. Queries Run | <input type="checkbox"/> | f. Contents of Files | <input type="checkbox"/> |
| 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 | <input type="checkbox"/> | Hard Copy: Mail/Fax | <input type="checkbox"/> | Online | <input checked="" type="checkbox"/> |
| Telephone | <input type="checkbox"/> | Email | <input type="checkbox"/> | | |
| Other(specify): | | | | | |

| | | | | | |
|---------------------------|-------------------------------------|-------------------|--------------------------|------------------------|--------------------------|
| Government Sources | | | | | |
| Within the Bureau | <input checked="" type="checkbox"/> | Other DOC Bureaus | <input type="checkbox"/> | Other Federal Agencies | <input type="checkbox"/> |
| State, Local, Tribal | <input type="checkbox"/> | Foreign | <input type="checkbox"/> | | |
| Other(specify): | | | | | |

| | | | | | |
|-------------------------------|--|--|--|--|--|
| Non-government Sources | | | | | |
|-------------------------------|--|--|--|--|--|

| | | | | | |
|------------------------------------|--------------------------|----------------|-------------------------------------|-------------------------|--------------------------|
| Public Organizations | <input type="checkbox"/> | Private Sector | <input checked="" type="checkbox"/> | Commercial Data Brokers | <input type="checkbox"/> |
| Third Party Website or Application | | | <input type="checkbox"/> | | |
| Other (specify): | | | | | |

2.3 Describe how the accuracy of the information in the system is ensured.

PCTSRS is an internal web docketing system that is only accessible by authenticated authorized employees. This system is not publicly 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 all access to PCT data. All data transfers between the USPTO and CIP are performed over encrypted connections which ensure confidentiality and data integrity.

2.4 Is the information covered by the Paperwork Reduction Act?

| | |
|-------------------------------------|--|
| <input checked="" type="checkbox"/> | Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. OMB control # 0651-0021 |
| <input type="checkbox"/> | No, the information is not covered by the Paperwork Reduction Act. |

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

| Technologies Used Containing PII/BII Not Previously Deployed (TUCPBND) | | | |
|--|--------------------------|--|--------------------------|
| Smart Cards | <input type="checkbox"/> | Biometrics | <input type="checkbox"/> |
| Caller-ID | <input type="checkbox"/> | Personal Identity Verification (PIV) Cards | <input type="checkbox"/> |
| Other (specify): | | | |

| | |
|-------------------------------------|--|
| <input checked="" type="checkbox"/> | There are not any technologies used that contain PII/BII in ways that have not been previously deployed. |
|-------------------------------------|--|

Section 3: System Supported Activities

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

| | | | |
|--------------------|--------------------------|----------------------------------|--------------------------|
| Activities | | | |
| Audio recordings | <input type="checkbox"/> | Building entry readers | <input type="checkbox"/> |
| Video surveillance | <input type="checkbox"/> | Electronic purchase transactions | <input type="checkbox"/> |
| Other (specify): | | | |

| | |
|-------------------------------------|--|
| <input checked="" type="checkbox"/> | There are not any IT system supported activities which raise privacy risks/concerns. |
|-------------------------------------|--|

Section 4: Purpose of the System

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

| | | | |
|--|-------------------------------------|--|-------------------------------------|
| Purpose | | | |
| For a Computer Matching Program | <input type="checkbox"/> | For administering human resources programs | <input type="checkbox"/> |
| For administrative matters | <input checked="" type="checkbox"/> | To promote information sharing initiatives | <input checked="" type="checkbox"/> |
| For litigation | <input type="checkbox"/> | For criminal law enforcement activities | <input type="checkbox"/> |
| For civil enforcement activities | <input type="checkbox"/> | For intelligence activities | <input type="checkbox"/> |
| To improve Federal services online | <input type="checkbox"/> | For employee or customer satisfaction | <input type="checkbox"/> |
| For web measurement and customization technologies (single-session) | <input type="checkbox"/> | For web measurement and customization technologies (multi-session) | <input type="checkbox"/> |
| Other (specify): USPTO collects, maintains, and disseminates the information with PCTRS that returns the completed document back to USPTO for consumption. | | | |

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).

| |
|--|
| <p>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. PCTRS is an internal web docketing system that is only accessible by authenticated and authorized employees. This system is not publicly accessible via the Internet.</p> |
|--|

- 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.)

Foreign entities, adversarial entities and insider threats are the predominant threats to the information collected and its privacy. The system has implemented security controls following NIST guidance to deter and prevent threats to privacy. CIP requires security awareness training, which covers appropriate handling of information, for all personnel at the time of hire, prior to granting access to the information system, and annually thereafter. The PCTSRS system automatically purges information in accordance with the retention schedule defined by the USPTO.

PE2E

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

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

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

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

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

| | |
|-------------------------------------|---|
| <input checked="" type="checkbox"/> | 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: PE2E |
| <input type="checkbox"/> | No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII. |

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

| Class of Users | | | |
|------------------|-------------------------------------|----------------------|-------------------------------------|
| General Public | <input type="checkbox"/> | Government Employees | <input checked="" type="checkbox"/> |
| Contractors | <input checked="" type="checkbox"/> | | |
| Other (specify): | | | |

Section 7: Notice and Consent

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

| | | |
|-------------------------------------|--|---|
| <input checked="" type="checkbox"/> | Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9. | |
| <input checked="" type="checkbox"/> | Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://www.uspto.gov/privacy-policy | |
| <input checked="" type="checkbox"/> | Yes, notice is provided by other means. | Specify how: Notice is provided at the time of collection by the Patent Capture and Application Processing System – Initial Processing (PCAPS-IP). |

| | | |
|--------------------------|-----------------------------|------------------|
| <input type="checkbox"/> | No, notice is not provided. | Specify why not: |
|--------------------------|-----------------------------|------------------|

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

| | | |
|-------------------------------------|---|--|
| <input checked="" type="checkbox"/> | Yes, individuals have an opportunity to decline to provide PII/BII. | Specify how: Applicants have the opportunity to decline to provide their PII/BII, this option is provided by PCAPS-IP. CIP PCTSRs does not collect data directly. |
| <input type="checkbox"/> | 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.

| | | |
|-------------------------------------|--|---|
| <input checked="" type="checkbox"/> | 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 the collection. This option is provided by PCAPS-IP. |
| <input type="checkbox"/> | 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.

| | | |
|-------------------------------------|---|---|
| <input checked="" type="checkbox"/> | Yes, individuals have an opportunity to review/update PII/BII pertaining to them. | Specify how: During patent submission via PCAPS-IP 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. |
| <input type="checkbox"/> | 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.)*

| | |
|-------------------------------------|--|
| <input checked="" type="checkbox"/> | All users signed a confidentiality agreement or non-disclosure agreement. |
| <input checked="" type="checkbox"/> | All users are subject to a Code of Conduct that includes the requirement for confidentiality. |
| <input checked="" type="checkbox"/> | Staff (employees and contractors) received training on privacy and confidentiality policies and practices. |
| <input checked="" type="checkbox"/> | Access to the PII/BII is restricted to authorized personnel only. |

| | |
|-------------------------------------|--|
| <input checked="" type="checkbox"/> | Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Audit Logs |
| <input checked="" type="checkbox"/> | The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 12/26/2023 <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved. |
| <input checked="" type="checkbox"/> | The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher. |
| <input checked="" type="checkbox"/> | NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 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). |
| <input checked="" type="checkbox"/> | A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks. |
| <input checked="" type="checkbox"/> | Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy. |
| <input checked="" type="checkbox"/> | Contracts with customers establish DOC ownership rights over data including PII/BII. |
| <input checked="" type="checkbox"/> | Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers. |
| <input type="checkbox"/> | Other (specify): |

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.
(Include data encryption in transit and/or at rest, if applicable).

PCTSRS is an internal web docketing system that is only accessible by authenticated and authorized employees. This system is not publicly 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 screened authorized employees who require this data to perform their job. The PCTSRS system logs all access to PCT data. Backup data is encrypted at rest and data encrypted during transmission.

Section 9: Privacy Act

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

☒ Yes, the PII/BII is searchable by a personal identifier.

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

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C.

§ 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

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

| | |
|-------------------------------------|--|
| <input checked="" type="checkbox"/> | Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. <i>(list all that apply):</i> PAT/TM—7 Patent Application Files |
| <input type="checkbox"/> | Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> . |
| <input type="checkbox"/> | No, this system is not a system of records and a SORN is not applicable. |

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

| | |
|-------------------------------------|---|
| <input checked="" type="checkbox"/> | There is an approved record control schedule. Provide the name of the record control schedule: Patent Examination Working Files (N1-241-10-1:4.2) |
| <input type="checkbox"/> | No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule: |
| <input type="checkbox"/> | Yes, retention is monitored for compliance to the schedule. |
| <input type="checkbox"/> | No, retention is not monitored for compliance to the schedule. Provide explanation: |

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

| Disposal | | | |
|------------------|-------------------------------------|-------------|-------------------------------------|
| Shredding | <input checked="" type="checkbox"/> | Overwriting | <input checked="" type="checkbox"/> |
| Degaussing | <input checked="" type="checkbox"/> | Deleting | <input type="checkbox"/> |
| 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.)*

| | |
|-------------------------------------|---|
| <input type="checkbox"/> | Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. |
| <input checked="" type="checkbox"/> | Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. |
| <input type="checkbox"/> | High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. |

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

| | | |
|-------------------------------------|---------------------------------------|---|
| <input checked="" type="checkbox"/> | Identifiability | Provide explanation: The combination of occupation, name, title, address, phone number, email address, and work address can be used to identify a particular individual. |
| <input checked="" type="checkbox"/> | Quantity of PII | Provide explanation: PCTSRs currently stores approximately 10,000 patent applications. Each patent application may contain the following PII: Inventor name, Inventor address, Citizenship, Correspondence address, Employer name and address, Telephone number[s], and E-mail address |
| <input checked="" type="checkbox"/> | Data Field Sensitivity | Provide explanation: Each patent application may contain the following PII: Inventor name, Inventor address, Citizenship, Correspondence address, Employer name and address, Telephone number(s), and E-mail address which together increases the sensitivity of the identifying data. |
| <input checked="" type="checkbox"/> | Context of Use | Provide explanation: Information is used to facilitate PCT searches by contractors working outside of the USPTO environment. |
| <input checked="" type="checkbox"/> | Obligation to Protect Confidentiality | Provide explanation: Based on the data fields and in accordance with the Privacy Act of 1974, PII must be protected and contract requirements. |
| <input checked="" type="checkbox"/> | 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. |
| <input type="checkbox"/> | Other: | Provide explanation: |

Section 12: Analysis

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

Foreign entities, adversarial entities and insider threats are the predominant threats to the information collected and its privacy. The system has implemented security controls following NIST guidance to deter and prevent threats to privacy. PCTSRS does not collect information from any sources other than the USPTO secure file transfer. CIP requires security awareness training, which covers appropriate handling of information, for all personnel at the time of hire, prior to granting access to the information system, and annually thereafter. The PCTSRS system automatically purges information in accordance with the retention schedule defined by the USPTO.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

| | |
|-------------------------------------|--|
| <input type="checkbox"/> | Yes, the conduct of this PIA results in required business process changes. Explanation: |
| <input checked="" type="checkbox"/> | No, the conduct of this PIA does not result in any required business process changes. |

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

| | |
|-------------------------------------|--|
| <input type="checkbox"/> | Yes, the conduct of this PIA results in required technology changes. Explanation: |
| <input checked="" type="checkbox"/> | No, the conduct of this PIA does not result in any required technology changes. |