

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



**Privacy Threshold Analysis
for the
Cardinal IP (CIP) Patent Cooperation Treaty Search Recordation
System (PCTSRS)**

U.S. Department of Commerce Privacy Threshold Analysis
Cardinal IP (CIP) Patent Cooperation Treaty Search Recordation System
(PCTSRS)

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

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose:

- (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 is 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 the USPTO Network Security Infrastructure (NSI) Enterprise Access Infrastructure System (EAIS).
- (d) The purpose that the systems is designed to serve*
PCTSRS facilitates PCT searches and written opinions on behalf of the USPTO.
- (e) The way the system operates to achieve the purpose*
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.
- (f) A general description of the type of information collected, maintained, use, or disseminated by the system*
The PII/BII collected consists of PCT patent applicant bibliographic data: Inventor name, Attorney name, Agent name, Company Name, Inventor address, Correspondence address, Citizenship, Telephone number, E-mail address, and application number.
- (g) Identify individuals who have access to information on the system*
Privileged Access: System Administrators and Subject Matter Expert Specialists. Non-privileged Access: Patent Researchers.
- (h) 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 TLS.

(i) *How information is transmitted to and from the system*

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

Questionnaire:

1. What is the status of this information system?

- ☐ This is a new information system. *Continue to answer questions and complete certification.*
- ☐ This is an existing information system with changes that create new privacy risks. *Complete chart below, 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):					

- ☐ 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. *Continue to answer questions and complete certification.*
- ☒ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

- ☐ Yes. *Please describe the activities which may raise privacy concerns.*
- ☒ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the

submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

☒ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

☒ Companies

☒ Other business entities

☐ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

☒ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

☐ DOC employees

☐ Contractors working on behalf of DOC

☒ Members of the public

☐ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

☒ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

☐ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

- ☐ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.
- ☒ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.

CERTIFICATION

☒ I certify the criteria implied by one or more of the questions above **apply** to the Cardinal IP Patent Cooperation Treaty Search Recordation System and as a consequence of this applicability, I will perform and document a PIA for this IT system.

☐ I certify the criteria implied by the questions above **do not apply** to the Cardinal IP Patent Cooperation Treaty Search Recordation System and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Blaine Copenheaver
Name of System Owner (SO): _____

Signature of SO: _____ Date: _____

Don Watson
Name of Chief Information Security Officer (CISO): _____

Signature of CISO: _____ Date: _____

Henry J. Holcombe
Name of Authorizing Official (AO) & Bureau Chief Privacy Officer (BCPO): _____

Signature of AO & BCPO: _____ Date: _____

Maria Holtmann
Name of Authorizing Official (AO) or Designated Representative: _____

Signature of AO: _____ Date: _____