

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



**Privacy Threshold Analysis
for the
Global Patent Solutions (GPS) System**

U.S. Department of Commerce Privacy Threshold Analysis

USPTO Global Patent Solutions (GPS) System

Unique Project Identifier: [2370] PTOC-024-00

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:

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

The GPS is a major application automated information system, and provides support to USPTO patent review process. It is exclusively dedicated for processing USPTO information. The system is physically located at a Tier IV data center, located at the ViaWest data center in Las Vegas, NV (3330 E Lone Mountain Rd, North Las Vegas, NV 89081).

GPS receives PCT application data from the USPTO via secure file transfer protocol using Tumbleweed, with an encrypted SSL connection. This data includes information to facilitate the patent application process, and comes from persons applying for patents through the USPTO. This can include PII such as bibliographic data like Inventor name, Inventor address, Citizenship, Correspondence address, Employer name and address, Telephone number[s], and E-mail address.

The purpose of this system is designed to support the USPTO international application or PCT application process. The GPS system facilitates PCT searches and enables GPS employees to submit an accompanying written opinion regarding the patentability of the invention in question. The system consists of a variety of document review, research tools, and case management software to facilitate the evaluation of and writing opinions on the PCT files provided by USPTO.

Only authorized GPS personnel have access to the system. PCT analysts perform assessments of USPTO PCT applications and have limited access to authorized files. Company managers, who supervise these employees and review their PCT application assessments, also have limited access to the system. System administrators have the highest privileges, to make changes on the network.

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 Global Patent Solutions (GPS) 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 Global Patent Solutions (GPS) system and as a consequence of this non-applicability, a PIA for this IT system is not necessary.


Name of System Owner (SO): Blaine Copenheaver

Signature of SO:  Date: 7-9-18

Name of Senior Information Security Officer (SISO): Rami Dillon

Signature of SISO:  Date: 7-11-18

Name of Authorizing Official (AO) & Bureau Chief Privacy Officer (BCPO): David Chiles

Signature of AO & BCPO:  Date: 7/16/2018

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

Signature of AO:  Date: 7/18/18