

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



**Privacy Threshold Analysis  
for the  
Patent Public Search (PPUBS)**

## U.S. Department of Commerce Privacy Threshold Analysis

### USPTO Patent Public Search (PPUBS)

**Unique Project Identifier: PTOC-055-00**

**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:** *Provide a brief description of the information system.*

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).

Patent Public Search (PPUBS) is a custom developed software application provided by the USPTO to allow the public to search U.S. patent documents in the USPTO databases. The PPUBS application is deployed in Amazon Web Services (AWS) and operates in an AWS virtual private cloud (VPC). It is a standalone application that does not interface with other USPTO or external information systems. The Patent text and image data provided to the public is a replica of examiner search collections used internally in USPTO.

Public access to PPUBS patent data is read-only. Access to PPUBS does not require user authentication. PPUBS inherits security groups from the USPTO AWS Cloud Services (UACS) authorization package and the Federal Risk and Authorization Management Program (FedRAMP) AWS US East/West Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) packages.

Address the following elements:

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

Patent Public Search System (PPUBS) is a Minor Application.

b) *System location*

USPTO Amazon Web Services (AWS) US East/West, Herndon, Virginia.

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

PPUBS interconnects with one other system:

**USPTO Amazon Cloud Services (UACS):** The UACS Infrastructure-as-a-Service (IaaS) platform used to support USPTO Application Information Systems (AIS) hosted in the Amazon Web Services (AWS) East/West environment. UACS leverages AWS Infrastructure-as-a-Service (IaaS) mode that enables on-demand Internet access to a shared pool of configurable computing resources including servers, storage, network infrastructure and other web-based services. The AWS East/West environment is comprised of several sub-components including, Virtual Private Cloud (VPC), Elastic Cloud Computing (EC2), Identity and Authentication Management (IAM), and Simple Storage Service.

*d) The purpose that the system is designed to serve*

PPUBS is the USPTO patent publications search system for public access and use.

*e) The way the system operates to achieve the purpose*

PPUBS is a patent search system for public use that is deployed and operating in the cloud.

*f) A general description of the type of information collected, maintained, used, or disseminated by the system*

PPUBS collects, maintains, and disseminates information about USPTO patents.

*g) Identify individuals who have access to information on the system*

The individuals who have access to PPUBS information are public users, internal USPTO patent examiners, and contractors.

*h) How information in the system is retrieved by the user*

Users use a web browser to view publicly provided information.

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

PPUBS transmits information to and from the system via client-server communication, which is protected by SSL encryption. User sessions are terminated when a set amount of inactivity is detected by the system.

## **Questionnaire:**

### **1. Status of the Information System**

#### **1a. 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	<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. *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. *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

- ☐ Yes. This is a new information system.
- ☐ Yes. This is an existing information system for which an amended contract is needed.
- ☐ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.
- ☒ No. This is not a new information system.

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. *(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):			

- ☒ 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.

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

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

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

☒ DOC employees

☒ Contractors working on behalf of DOC

☐ Other Federal Government personnel

☒ 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 Social Security numbers (SSNs), including truncated form?

☐ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.

Provide the legal authority which permits the collection of SSNs, including truncated form.

- ☒ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. 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.

4d. 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, 4c, and/or 4d are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the IT system’s Assessment and Authorization Package.***

## CERTIFICATION

☒ The criteria implied by one or more of the questions above **apply** to the Patent Public Search (PPUBS) and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

☐ The criteria implied by the questions above **do not apply** to the Patent Public Search (PPUBS) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

<b>System Owner</b> Name: Quast Elizabeth A. Office: P/OPA--OITP - OFFICE OF PATENT AUTOMATION Phone: (571) 272-2246 Email: Elizabeth.Quast@uspto.gov  Signature: _____ Date signed: _____	<b>Chief Information Security Officer</b> Name: Goodwin Timothy Scott Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-0653 Email: Timothy.Goodwin@uspto.gov  Signature: _____ Date signed: _____
<b>Privacy Act Officer</b> Name: Kyu Lee Office: Office of General Law (O/GL) Phone: (571) 272-6421 Email: Kyu.Lee@uspto.gov  Signature: _____ Date signed: _____	<b>Bureau Chief Privacy Officer and Co-Authorizing Official</b> Name: Henry J. Holcombe Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-9400 Email: Jamie.Holcombe@uspto.gov  Signature: _____ Date signed: _____
<b>Co-Authorizing Official</b> Name: Vaishali Udupa Office: Office of the Commissioner for Patents Phone: (571) 272-8800 Email: Vaishali.Udupa@uspto.gov  Signature: _____ Date signed: _____	