Template Version Number: 01-2021

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

Privacy Threshold Analysis
for the
Patent Capture and Application Processing System– Examination Support (PCAPS-ES)

U.S. Department of Commerce Privacy Threshold Analysis

USPTO Patent Capture and Application Processing System– Examination Support (PCAPS-ES)

Unique Project Identifier: PTOP-005-00

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).

The purpose of PCAPS-ES is to transmit and store data and images in support of the United States Patent and Trademark Office's (USPTO's) patent application process and its data capture and conversion requirements.

Address the following elements:

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

b) *System location*

600 Dulany Street, Alexandria, VA 22314

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

DBS (Database Services): The DBS is an infrastructure information system, and provides a database infrastructure to support USPTO database needs.

EDP (Enterprise Desktop Platform): The EDP is an infrastructure information system that provides a standard enterprise-wide environment that manages desktops and laptops running

on the Windows operating system (OS), providing United States Government Configuration Baseline (USGCB) compliant workstations.

ESS (Enterprise Software System): Provides Enterprise Directory Services (EDS), Role-Based Access Control (RBAC), Email as a Service (EaaS), PTO Exchange Services, Symantec Endpoint Protection, Enterprise SharePoint Services, etc.

EUS (Enterprise UNIX Services): The EUS system consists of assorted UNIX operating system (OS) variants, each comprised of many utilities along with the master control program, the kernel.

EWS (Enterprise Windows Services): The EWS is an infrastructure information system, and provides a hosting platform for major applications that support various USPTO missions.

IDSS (Information Dissemination Support System): The purpose of the IDSS system is to support the Trademark and Electronic Government Business Division, the Corporate Systems Division (CSD), the Patent Search System Division, the Office of Electronic Information Products, and the Office of Public Information Services. It provides automated support for the timely search and retrieval of electronic text and images concerning patent applications and patents by USPTO internal and external users.

IPLMSS (Intellectual Property Leadership Management Support System): The IPLMSS is a system, which provides Adjudicated Case Tracking System, Electronic Freedom of Information Act System, Electronic System for Trademark Trials and Appeals, , General Counsel Case Tracking System, General Counsel Library System, Office of Enrollment and Discipline Item Bank, Office of Enrollment and Discipline Information System, Trademark Trial and Appeal Board, Trademark Trial and Appeal Board Information System, E-Discovery Software Suite, and NOSPS.

National Finance Center (NFC): NFC is a USDA personnel and payroll system.

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

PCAPS-IP (Patent Capture and Application Processing System – Capture and Initial Processing): PCAPS-IP is a system which provides support to the USPTO for the purposes of capturing patent applications and related metadata in electronic form; processing applications electronically; reporting patent application processing and prosecution status;

and retrieving and displaying patent applications. PCAPS-IP is comprised of multiple subsystems that perform specific functions, including submissions, categorization, metadata capture, and patent examiner assignment of patent applications.

PDDM (Patent Data and Document Management): PDDM is an off-site multi-vendor system that captures critical fields from applicant's applications so that they are pre-loaded into an index file to reduce examiners and public search times.

PE2E (Patent End to End): Patents End-to-End (PE2E) is a system consisting of next generation subsystems. The goal of PE2E is to make the interaction of USPTO's users as simple and efficient as possible in order to accomplish user goals. PE2E is a single web-based examination tool providing users with a unified and robust set of tools. PE2E has and will replace old and outdated legacy systems.

PSS-PS (Patent Search System – Primary Search and Retrieval): PSS-PS is a system consisting of multiple subsystems. PSS-PS supports legal determination of prior art for patent applications, including text and image search of repositories of US and foreign applications and granted publications, various concordances, and non-patent literature. It represents the databases that contain the images and text data for US patent grants, published applications, and unpublished applications.

RAM (Revenue Accounting and Management System): RAM is a system that collects fees for all USPTO goods and services related to intellectual property. While the FPNG system provides secure web applications from which internet customers can pay fees, FPNG forwards those payments to RAM to be processed and recorded. Fees submitted to the USPTO by mail are processed through the RAM desktop application by designated USPTO staff. Collected payment information is shared with the U.S. Treasury's Pay.gov system for credit card and ACH verification and processing.

SCS (Security and Compliance Services): Provides Security Incident and Event Management, Enterprise Forensic, Enterprise Management System, Security and Defense, Enterprise Scanner, Enterprise Cybersecurity Monitoring Operations, Performance Monitoring Tools, Dynamic Operational Support Plan, & Situational Awareness and Incident Response. SCS does not collect, maintain, and disseminate PII/BII.

SOI (Service Oriented Infrastructure): The SOI provides a feature-rich and stable platform upon which USPTO applications can be deployed.

TRINET (Trilateral Network): TRINET is an infrastructure information system and provides secure network connectivity for electronic exchange and dissemination of sensitive

patent data between authenticated endpoints at the Trilateral Offices and TRINET members. The Trilateral Offices consist of the United States Patent and Trademark Office (USPTO), the European Patent Office (EPO), and the Japanese Patent Office (JPO). The TRINET members consist of the World Intellectual Property Office (WIPO), the Canadian Intellectual Property Office (CIPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO) and the Intellectual Property Office of Australia (IPAU).

d) The purpose that the system is designed to serve

PCAPS-ES allows the submission, categorization, metadata capture, and Patent Examiner assignment of patent applications from internal and external customers of the USPTO.

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

PCAPS-ES uses several subsystems that allow the submission, categorization, metadata capture, and Patent Examiner assignment of patent applications from internal and external customers of the USPTO. It supports the Patent Business Function of USPTO.

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

- Published patent data
- Unpublished patent data
- Customer PII
- Employee PII
- Contractor PII

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

Individuals that have access to the system are: members of the public, USPTO Patent Examiners, USPTO patents and contractor employees, and foreign patent examiners.

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

- Public internet websites
- Internal web applications on PTONet

i) How information is transmitted to and from the system

For internal USPTO communication, transmission integrity is provided by internal access controls, firewalls, and VPN. Device management connections are protected by Secure Shell (SSH) based encrypted connections. PCAPS-ES data transmission is protected by the PTONet infrastructure.

For external connections to the DMZ, Contractor Access Zone (CAZ), and/or external networks, device management connections use SSH and Secure ID VPN-based connections. User data connections use Secure ID VPN and SSL/TLS. Additional session-level communication protection mechanisms are not utilized within PCAPS-ES. Limited session confidentiality is provided by the PTONet Local Area Network (LAN). Only authorized USPTO systems may access the internal PTONet.

Public users transmit information to and from Public PAIR and Private PAIR via HTTPS.

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	☐	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. *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	☐	Building entry readers	☐
Video surveillance	☐	Electronic purchase transactions	☐
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. PCAPS-ES uses SSNs, which are cross-referenced to USPTO HR assigned employee ID. Federal employee SSN are 9-digits and contractors are the last two digits of the SSN. Federal employee SSN are mandatory key identifiers that facilitate federal personnel data synchronization between USPTO HR payroll and the National Finance Center (NFC) only. The contractor's last two digits of the SSN are minimum administrative requirements for unique employee ID assignment. These fields are restricted only a select admin group. The assigned Employee ID is utilized within USPTO as a unique reference to identify USPTO employees, examiner actions, back office actions, etc. Sensitive PII is obfuscated (masked) when viewed directly by unauthorized viewers, such as administrators.
Provide the legal authority which permits the collection of SSNs, including truncated form. Executive Order 9397, 35 U.S.C. 1 and 115; 5 U.S.C. 301.

☐ 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 Capture and Application Processing System– Examination Support (PCAPS-ES) 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 Capture and Application Processing System– Examination Support (PCAPS-ES) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

System Owner Name: Michael Newman Office: Office of Patent Information Management (P/OPIM) Phone: (571) 270-3016 Email: Michael.Newman@uspto.gov Signature: Digitally signed by Users, Newman, Michael A. (OITP) Date: 2023.04.03 22:24:47 -04'00' Date signed: _____	**Chief Information Security Officer** Name: Don Watson Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-8130 Email: Don.Watson@uspto.gov Signature: Users, Watson, Don Digitally signed by Users, Watson, Don Date: 2023.04.14 08:46:15 -04'00' Date signed: _____
Privacy Act Officer Name: Ezequiel Berdichevsky Office: Office of General Law (O/GL) Phone: (571) 270-1557 Email: Ezequiel.Berdichevsky@uspto.gov Signature: Users, Berdichevsky, Ezequiel Digitally signed by Users, Berdichevsky, Ezequiel Date: 2023.04.10 09:28:19 -04'00' Date signed: _____	**Bureau Chief Privacy Officer and Co-Authorizing Official** Name: Henry J. Holcombe Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-9400 Email: Jamie.Holcombe@uspto.gov Signature: Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry Date: 2023.04.14 11:28:11 -04'00' Date signed: _____
Co-Authorizing Official Name: Vaishali Udupa Office: Office of the Commissioner of Patents Phone: (571) 272-8800 Email: Vaishali.Udupa@uspto.gov Signature: Users, Seidel, Richard Digitally signed by Users, Seidel, Richard Date: 2023.04.15 09:25:56 -04'00' Date signed: _____	