Version Number: 01-2017

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

Privacy Threshold Analysis
for the
Patent Search System – Primary Search & Retrieval (PSS-PS) System

U.S. Department of Commerce Privacy Threshold Analysis

USPTO Patent Search System – Primary Search & Retrieval (PSS-PS)

Unique Project Identifier: PTOP-008-00

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: *Provide a general description of the information system in a way that a non-technical person can understand.*

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).

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)*

Enterprise Windows Services (EWS): The EWS is an Infrastructure information system, and provides a hosting platform for major applications that support various USPTO missions.
Enterprise UNIX Services (EUS): The EUS System consists of assorted UNIX operating system variants (OS) each comprised of many utilities along with the master control program, the kernel.
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 United States Patent and Trademark Office (USPTO) IT applications.
Patent Capture and Application Processing System – Initial Processing (PCAPS-IP): The PCAPS-IP is an Application information system, and 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 Automated Information Systems (components) that perform specific functions, including submissions, categorization, metadata capture, and patent examiner assignment of patent applications.

Patent Capture and Application Processing System – Examination Support (PCAPS-ES): The PCAPS-ES is an Application information system, composed of 20 Components: Electronic Business Center Imaging System, Electronic Desktop Application Navigator, File Inspection Utility, Image File Wrapper, Office Action Correspondence System, Patent Resource Management System, PAIR User Resource Manager, Patent Application Location Monitoring – Examination and Post-Examination, Patent Application Location Monitoring – Services Gateway, Patent Application Location Monitoring – File Ordering System, Patent Application Location Monitoring- Infrastructure, Patent Application Information Retrieval-Private, Patent Enterprise Access Integration Public Patent Application Information Retrieval – Public, Trilateral Document Access, Patent File Wrapper, Quality Review System, Supplemental Complex Repository for Examiners, Technology Assessment and Forecast, Patents Telework Enterprise System, & Integrated Quality System.

Enterprise Desktop Platform (EDP): The EDP is an infrastructure information system that provides a standard enterprise-wide environment that manages desktops and laptops, providing United States Government Configuration Baseline (USGCB) compliant workstations.

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

Enterprise Software System (ESS): Provides Enterprise Directory Services, Role-Based Access Control System, Email as a Service, Anti-Virus, etc.

Enterprise Monitoring and Security Operations (EMSO): 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.

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

Trilateral Network (TRINET): 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).

Patent End to End (PE2E): Patents End-to-End (PE2E) is a Master system portfolio consisting of next generation Patents Automated Information Systems (AIS). 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 will be a single web-based examination tool providing users with a unified and robust set of tools. PE2E will overhaul the current patents examination baseline through the development of a new system that replaces the existing tools used in the examination process.

Data Storage Management System (DSMS): DSMS is an infrastructure system that provides archival and storage capabilities securely to the USPTO. The information system is considered an essential component of USPTO's Business Continuity and Disaster Recovery program. DSMS consists of the following subsystems: Data Capture System, Enterprise Tape Backup System, Storage Infrastructure System.

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

Patent Search System - Primary Search and Retrieval (PSS-PS) supports legal determination of prior art for patent applications, including text and image search of repositories of US application and grant publications, Foreign application and grant 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. This area includes the examiner interfaces that provide the search capability through East and West.

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

The PSS-PS master system has multiple AISs with search and retrieval automation tools that supports the USPTO Patent examiners legal determination of prior art of patent applications.

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

Published patent data.

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

Public and USPTO patent examiners.

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

Public internet websites and internal applications.

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, PKI, and Secure ID VPN-based connections. User data connections use PKI and 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.

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.*

_X__ 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.*

_X__ 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.)."

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

_X__ Companies
_X__ 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..."

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

__ X _ DOC employees
___ Contractors working on behalf of DOC
___X 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?

_ X _ 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.

_X__ 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 PSS-PS. This PTA and the approved PIA must be a part of the PSS-PS's Assessment and Authorization Package.

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the PSS-PS 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 PSS-PS and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO): _____William Stryjewski_____

Signature of ISSO or SO: _____ Date: 8/5/19

Name of Senior Information Security Officer (SISO): ____Don Watson_____

Signature of SISO: _____ Date: 8/12/19

Name of Co-Authorizing Official (AO)/Bureau Chief Privacy Officer (BCPO)
_____Henry J. Holcombe____

Signature of Co-AO/BCPO_____ Date: 15 AUG '19

Name of Co-Authorizing Official (Co-AO): ____Richard Seidel_____

Signature of Co-AO: _____ Date: 08/20/2019