

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



**Privacy Threshold Analysis
for the
Patent End to End (PE2E) System**

U.S. Department of Commerce Privacy Threshold Analysis

USPTO Patent End to End (PE2E)

Unique Project Identifier: PTOP-003-00

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*

PE2E is a major applications consisting of multiple applications.

b) *System location*

Madison building 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)*

PE2E interconnects with the following:

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

Enterprise Desktop Platform (EDP): is an infrastructure information system which provides a standard enterprise-wide environment that manages desktops and laptops running on the Windows 7 and Windows 10 operating system (OS), providing United States Government Configuration Baseline (USGCB) compliant workstations. The USGCB security mandate by the Office of Management and Budget (OMB) requires all Federal Agencies, including the USPTO, to use the directed desktop configuration.

Enterprise Monitoring and Security Operations (EMSO): - The SIEM provides a centralized command and control console with integrated enterprise log management, security information and event management, network behavior analysis, and reporting through the collection of events, network/application flow data, vulnerability data, and identity information.

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

Network and Security Infrastructure (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.

Enterprise Software Services (ESS): is an Infrastructure information system and provides a variety services to support USPTO missions.

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

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.

Reed Technology and Information Services (RTIS) Patent Data Capture (PDCap)/SERCO Patent Processing System (PPS); RTIS is an off-campus contractor 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. SERCO PPS is a contractor system that receives information from USPTO so that inventory, identification and classification activities can be performed on patent applications.

Patent Capture and Application Processing System – Examination Support (PCAPS ES): is a master system that provides a comprehensive prior art search capability and the retrieval of patent and related information, which comprise text and images of United States (US), European Patent Office (EPO) and Japan Patent Office (JPO patents), US pre-grant publications, Derwent data and IBM Technical Disclosure Bulletins.

Patent Capture and Application Processing System – Initial Processing (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.

Patent Search System – Primary Search and Retrieval (PSS PS): is a master system that processes, transmits and store data and images to support the data-capture and conversion requirements of the USPTO to support the USPTO patent application process.

Patent Search System – Specialized Search and Retrieval (PSS SS): The PSS-SS system is made up of multiple applications that allow Patents examiners and applicants to effectively search the USPTO Patent data repositories.

Service Orientated Infrastructure (SOI): is an infrastructure system that provides a

feature-rich and stable platform upon which USPTO applications can be deployed.

Data Storage Management System (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.

d) The purpose that the system is designed to serve

Patent End to End (PE2E) is a Master system portfolio consisting of next generation Patents Automated Information Systems (AISs) which process applications for the issuance and granting of U.S. Patents. 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.

e) The way the system operates to achieve the purpose

PE2E will be a single web-based examination tool providing users with a unified and robust set of tools.

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

Published and unpublished Patents data

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

Public, Patent Examiner, Legal Instruments Examiners (LIEs), system administrators, PTONet Internal Users, Foreign Offices – JPO, KIPO, SIPO, EPO

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

Registered patent applicants are provisioned unique user accounts to facilitate subsequent secure logins for their application status and update submissions. Patent examiners are granted access only the patent application has been assigned to them.

i) How information is transmitted to and from the system

HTTPS is used for all data transmissions to and from the Internet, USPTO DMZ, and PTONet. A dedicated socket is used to perform encryption and decryption.

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.

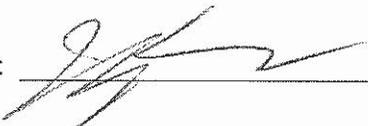
If any of the answers to questions 2, 3, 4b, and/or 4c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.

CERTIFICATION

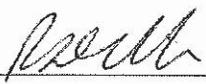
 X I certify the criteria implied by one or more of the questions above **apply** to the PE2E and as a consequence of this applicability, I will perform and document a PIA for this IT system.

 I certify the criteria implied by the questions above **do not apply** to the PE2E 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: 8/23/18

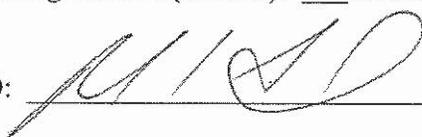
Name of Senior Information Security Officer (SISO): Rami Dillon

Signature of SISO:  Date: 8/28/18

Name of Authorizing Official (AO)/Bureau Chief Privacy Officer (BCPO) ^{for} David Chiles

Signature of AO/BCPO  Dep OCIO Date: 8/31/18

Name of Co-Authorizing Official (Co-AO): Richard Seidel

Signature of Co-AO:  Date: 9/4/2018