Template Version Number: 01-2021

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

Privacy Threshold Analysis
for the
Trilateral Network (TRINET)

U.S. Department of Commerce Privacy Threshold Analysis

USPTO Trilateral Network (TRINET)

Unique Project Identifier: EIPL-IHSN-07-00

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).

TRINET disseminates unpublished patent application information and priority documents in regards to the application process. TRINET is an Infrastructure information system, and provides secure network connectivity for electronic exchange and dissemination of 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) and the Korean Intellectual Property Office (KIPO). All members sign an MOU agreement to share patent information through end user access and credentials provided by USPTO TRINET.

Address the following elements:

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

b) System location
TRINET is located in Alexandria, VA.

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
TRINET has the following interconnections:

European Patent Office (EPO): The EPO is the European Patent Office that examines European Patent applications including its member states and provides secure network connectivity for electronic exchange and dissemination of sensitive patent data between

authenticated access points at the Trilateral Offices and TRINET members.

Japan Patent Office (JPO): The JPO is the Japan Patent Office that examines Japan Patent applications and Intellectual Property services and provides secure network connectivity for electronic exchange and dissemination of sensitive patent data between authenticated access points at the Trilateral Offices and TRINET members.

Korean Intellectual Property Office (KIPO): The KIPO is the Korean Intellectual Property Office that Examines Korean Patent applications and Intellectual Property services and provides secure network connectivity for electronic exchange and dissemination of sensitive patent data between authenticated access points at the Trilateral Offices and TRINET members.

World Intellectual Property Organization (WIPO): The WIPO is the World Intellectual Property Organization, a United Nations organization processing Intellectual Property services, which provides secure network connectivity for electronic exchange and dissemination of sensitive patent data between authenticated access points at the Trilateral Offices and TRINET members.

Network and Security Infrastructure (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.

Security and Compliance Services (SCS): The Security and Compliance Services system provides automated, proactive system management, and service-level management for network devices and application and database servers.

Enterprise UNIX Services (EUS): The EUS is an infrastructure operating system with a sole purpose of providing a UNIX base hosting platform to support other systems at USPTO.

Enterprise Software Services (ESS): Enterprise Software Services system provides the USPTO organization with a collection of programs that utilize common business applications and tools for modeling how the entire organization works.

Patent End to End (PE2E): Patent End to End (PE2E) is a next generation major application that collects patent application submissions (online and paper copy) from patent applicants (inventors) or their legal representative for examination, granting and issuance of U.S. Patents.

Patent Capture and Application Processing System – Examination Support (PCAPS-ES): The PCAPS-ES is an Application Information System (AIS) composed of 19 components to provide patent capture and application processing capabilities and functionality.

Patent Capture and Application Processing System – Capture and Initial Processing (PCAPS-IP): PCAPS-IP is an Application Information System that provides support 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 Search System – Primary Search and Retrieval (PSS-PS): is a major system, which supports the Patent Cost Center. It is considered a mission critical "system." It consist of Search and Retrieval automation tools that provide 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.

d) The purpose that the system is designed to serve

TRINET provides secure network connectivity for electronic exchange and dissemination of patent data between authenticated endpoints at the Trilateral Offices and TRINET members.

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

TRINET is essentially a 'conduit' that provides connectivity to a well-defined set of USPTO applications and resources based on user roles and functions. The connections within TRINET are between systems within the foreign Intellectual Property Offices (EPO, JPO, KIPO, WIPO). TRINET contains a security enclave (IDSSC) that creates a secure DMZ in which international offices can access information without directly accessing other internal networks.

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

Information collected from members of the public supports business processes and creates efficiencies for customers to protect their intellectual property (IP) rights.

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

h) How information in the system is retrieved by the user
TRINET users receive information through Secure File Transfer Protocol. Additionally, USPTO implements NIST security controls for user access, to include but not limited to two-factor authentication.

i) How information is transmitted to and from the system
TRINET transmits information between international patent partners using a Point-to-Point dedicated Virtual Private Network (VPN). No sensitive PII is transmitted.

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.
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 Trilateral Network (TRINET) 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 Trilateral Network (TRINET) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

System Owner Name: Edison Lewark Office: Infrastructure Services Division (I/ISD) Phone: (571) 272-8568 Email: Edison.Lewark@uspto.gov Signature: Edison Lewark Digitally signed by Edison Lewark Date: 2023.10.23 09:45:05 -04'00' Date signed: _____	**Chief Information Security Officer** Name: Timothy S. Goodwin Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-0653 Email: Timothy.Goodwin@uspto.gov Signature: Timothy S. Goodwin Digitally signed by Users, Goodwin, Timothy Date: 2023.10.27 14:00:50 -04'00' Date signed: _____
Privacy Act Officer Name: Heaton John Office: Office of General Law (O/GL) Phone: (703) 756-1240 Email: Ricou.Heaton@uspto.gov Signature: John Ricou Heaton Digitally signed by John Ricou Heaton Date: 2023.10.19 16:25:07 -04'00' Date signed: _____	**Bureau Chief Privacy Officer and 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: 2023.10.27 21:29:12 -04'00' Date signed: _____
Co-Authorizing Official Name: N/A Office: N/A Phone: N/A Email: N/A Signature: _____ Date signed: _____	