

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



**Privacy Impact Assessment
for the
Trilateral Network (TRINET)**

Reviewed by: Henry J. Holcombe, Bureau Chief Privacy Officer

- ☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry
Date: 2022.10.04 13:14:30 -04'00'

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Date

U.S. Department of Commerce Privacy Impact Assessment USPTO Trilateral Network (TRINET)

Unique Project Identifier: EIPL-IHSN-07-00

Introduction: System Description

Provide a brief description of the information system.

TRINET disseminates unpublished patent application information and priority documents in regards to the application process.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

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)

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 way the system operates to achieve the purpose(s) identified in Section 4

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.

(e) 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.

(f) 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.

(g) Any information sharing

The information is shared with the foreign Intellectual Property (IP) Offices (EPO, JPO, KIPO, and WIPO).

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

35 U.S.C. 2, 115, 117, 118, 122, 184, 261, 371; 37 C.F.R. 1.14

- (i) *The Federal Information Processing Standards (FIPS) 199 security impact category for the system*

Moderate

Section 1: Status of the Information System

- 1.1 Indicate whether the information system is a new or existing system.

☐ This is a new information system.

☐ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

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.

☒ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

- 2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*	<input type="checkbox"/>	f. Driver's License	<input type="checkbox"/>	j. Financial Account	<input type="checkbox"/>
b. Taxpayer ID	<input type="checkbox"/>	g. Passport	<input type="checkbox"/>	k. Financial Transaction	<input type="checkbox"/>
c. Employer ID	<input type="checkbox"/>	h. Alien Registration	<input type="checkbox"/>	l. Vehicle Identifier	<input type="checkbox"/>
d. Employee ID	<input type="checkbox"/>	i. Credit Card	<input type="checkbox"/>	m. Medical Record	<input type="checkbox"/>
e. File/Case ID	<input checked="" type="checkbox"/>				
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

--

General Personal Data (GPD)					
a. Name	<input checked="" type="checkbox"/>	h. Date of Birth	<input type="checkbox"/>	o. Financial Information	<input type="checkbox"/>
b. Maiden Name	<input type="checkbox"/>	i. Place of Birth	<input type="checkbox"/>	p. Medical Information	<input type="checkbox"/>
c. Alias	<input type="checkbox"/>	j. Home Address	<input checked="" type="checkbox"/>	q. Military Service	<input type="checkbox"/>
d. Gender	<input type="checkbox"/>	k. Telephone Number	<input checked="" type="checkbox"/>	r. Criminal Record	<input type="checkbox"/>
e. Age	<input type="checkbox"/>	l. Email Address	<input checked="" type="checkbox"/>	s. Marital Status	<input type="checkbox"/>
f. Race/Ethnicity	<input type="checkbox"/>	m. Education	<input type="checkbox"/>	t. Mother's Maiden Name	<input type="checkbox"/>
g. Citizenship	<input checked="" type="checkbox"/>	n. Religion	<input type="checkbox"/>		
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	<input type="checkbox"/>	e. Work Email Address	<input checked="" type="checkbox"/>	i. Business Associates	<input type="checkbox"/>
b. Job Title	<input type="checkbox"/>	f. Salary	<input type="checkbox"/>	j. Proprietary or Business Information	<input checked="" type="checkbox"/>
c. Work Address	<input checked="" type="checkbox"/>	g. Work History	<input type="checkbox"/>	k. Procurement/contracting records	<input type="checkbox"/>
d. Work Telephone Number	<input checked="" type="checkbox"/>	h. Employment Performance Ratings or other Performance Information	<input type="checkbox"/>		
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	<input type="checkbox"/>	f. Scars, Marks, Tattoos	<input type="checkbox"/>	k. Signatures	<input type="checkbox"/>
b. Palm Prints	<input type="checkbox"/>	g. Hair Color	<input type="checkbox"/>	l. Vascular Scans	<input type="checkbox"/>
c. Voice/Audio Recording	<input type="checkbox"/>	h. Eye Color	<input type="checkbox"/>	m. DNA Sample or Profile	<input type="checkbox"/>
d. Video Recording	<input type="checkbox"/>	i. Height	<input type="checkbox"/>	n. Retina/Iris Scans	<input type="checkbox"/>
e. Photographs	<input type="checkbox"/>	j. Weight	<input type="checkbox"/>	o. Dental Profile	<input type="checkbox"/>
p. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	<input type="checkbox"/>	c. Date/Time of Access	<input type="checkbox"/>	e. ID Files Accessed	<input type="checkbox"/>
b. IP Address	<input type="checkbox"/>	f. Queries Run	<input type="checkbox"/>	f. Contents of Files	<input type="checkbox"/>
g. Other system administration/audit data (specify):					

Other Information (specify)					

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	<input type="checkbox"/>	Hard Copy: Mail/Fax	<input checked="" type="checkbox"/>	Online	<input checked="" type="checkbox"/>
Telephone	<input type="checkbox"/>	Email	<input type="checkbox"/>		
Other(specify):					

Government Sources					
Within the Bureau	<input checked="" type="checkbox"/>	Other DOC Bureaus	<input checked="" type="checkbox"/>	Other Federal Agencies	<input checked="" type="checkbox"/>
State, Local, Tribal	<input checked="" type="checkbox"/>	Foreign	<input checked="" type="checkbox"/>		
Other(specify):					

Non-government Sources					
Public Organizations	<input type="checkbox"/>	Private Sector	<input checked="" type="checkbox"/>	Commercial Data Brokers	<input type="checkbox"/>
Third Party Website or Application			<input type="checkbox"/>		
Other(specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

<p>The system is secured using appropriate administrative physical and technical safeguards in accordance with the National Institute of Standards and Technology (NIST) security controls (encryption, access control, and auditing). Mandatory IT awareness and role-based training is required for staff who have access to the system and address how to handle, retain, and dispose of data. All access has role-based restrictions and individuals with privileges have undergone vetting and suitability screening. The USPTO maintains an audit trail and performs random, periodic reviews (quarterly) to identify unauthorized access and changes as part of verifying the integrity of administrative account holder data and roles. Inactive accounts will be deactivated and roles will be deleted from the application.</p> <p>Individuals can submit new documents to USPTO that would replace the existing PII/BII pertaining to them.</p>
--

2.4 Is the information covered by the Paperwork Reduction Act?

<input checked="" type="checkbox"/>	<p>Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.</p> <p>The data process by this system is collected under the following OMB control numbers: 0651-0031 Patent Processing 0651-0071 Matters Related to First Inventor to File</p>
<input type="checkbox"/>	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards	<input type="checkbox"/>	Biometrics	<input type="checkbox"/>
Caller-ID	<input type="checkbox"/>	Personal Identity Verification (PIV) Cards	<input type="checkbox"/>
Other(specify):			

<input checked="" type="checkbox"/>	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.
-------------------------------------	--

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(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): Click or tap here to enter text.			

<input checked="" type="checkbox"/>	There are not any IT systems supported activities which raise privacy risks/concerns.
-------------------------------------	---

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program	<input type="checkbox"/>	For administering human resources programs	<input type="checkbox"/>
For administrative matters	<input checked="" type="checkbox"/>	To promote information sharing initiatives	<input checked="" type="checkbox"/>
For litigation	<input type="checkbox"/>	For criminal law enforcement activities	<input type="checkbox"/>
For civil enforcement activities	<input type="checkbox"/>	For intelligence activities	<input type="checkbox"/>
To improve Federal services online	<input type="checkbox"/>	For employee or customer satisfaction	<input type="checkbox"/>
For web measurement and customization technologies (single-session)	<input type="checkbox"/>	For web measurement and customization technologies (multi-session)	<input type="checkbox"/>
Other(specify): For international patent treaties (Paris Convention, Patent Cooperation Treaty (PCT), the Hague, etc.			

Section 5: Use of the Information

- 5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

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

The information is disseminated at the explicit request of the applicants to support the examination of patent applications (global filing) pending at other IP Offices.

- 5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

In the event of computer failure, insider threats, or attack against the system by adversarial or foreign entities, any potential PII data stored within the system could be exposed. To avoid a breach, the system has certain security controls in place to ensure the information is handled, retained, and disposed of appropriately. Access to individual's PII is controlled through the application, and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. These audit trails are based on application server out-of-the-box logging reports reviewed by the Information System Security Officer (ISSO) and System Auditor and any suspicious indicators such as browsing will be immediately investigated and appropriate action taken. Also, system users undergo annual mandatory training regarding appropriate handling of information.

NIST security controls are in place to ensure that information is handled, retained, and disposed of appropriately. For example, advanced encryption is used to secure the data both during transmission and while stored at rest. Access to individual's PII is controlled through the application. All personnel who access the data must provide authentication to access the system. An audit trail is generated when the database is accessed. These audit trails are based on application server out-of-the-box logging reports reviewed by the Information System Security Officer (ISSO) and System Auditor. Any suspicious indicators are immediately investigated and appropriate action is taken, if necessary. System users undergo annual mandatory training regarding appropriate handling of information.

Section 6: Information Sharing and Access

- 6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DOC bureaus	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Federal agencies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
State, local, tribal gov't agencies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Private sector	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign governments	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign entities	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other(specify): Foreign IP Offices	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

<input type="checkbox"/>	The PII/BII in the system will not be shared.
--------------------------	---

- 6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

<input type="checkbox"/>	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
<input checked="" type="checkbox"/>	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
<input type="checkbox"/>	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

- 6.3 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

<input checked="" type="checkbox"/>	<p>Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:</p> <p>Patent End to End (PE2E) Patent Capture and Application Processing System (PCAPS-IP) Patent Capture and Application Processing System (PCAPS-ES) Enterprise Software Services (ESS) Patent Search System– Primary Search and Retrieval (PSS-PS) Security and Compliance Services (SCS)</p> <p>NIST security controls are in place to ensure that information is handled, retained, and disposed of appropriately. For example, advanced encryption is used to secure the data both during transmission and</p>
-------------------------------------	--

	while stored at rest. Access to individual's PII is controlled through the application. All personnel who access the data must provide authentication to access the system. An audit trail is generated when the database is accessed. These audit trails are based on application server out-of-the-box logging reports reviewed by the Information System Security Officer (ISSO) and System Auditor. Any suspicious indicators are immediately investigated and appropriate action is taken, if necessary. System users undergo annual mandatory training regarding appropriate handling of information.
<input type="checkbox"/>	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public	<input type="checkbox"/>	Government Employees	<input checked="" type="checkbox"/>
Contractors	<input checked="" type="checkbox"/>		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

<input checked="" type="checkbox"/>	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
<input checked="" type="checkbox"/>	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://www.uspto.gov/privacy-policy	
<input checked="" type="checkbox"/>	Yes, notice is provided by other means.	Specify how: USPTO has a warning banner. A notice is provided by a warning banner when the applicant accesses the TRINET system to submit the information. Please see "APPENDIX A" for details on the warning banner.
<input type="checkbox"/>	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

<input checked="" type="checkbox"/>	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Individuals may decline to provide PII by not submitting an application for processing.
<input type="checkbox"/>	No, individuals do not have an opportunity to decline to provide	Specify why not:

	PII/BII.	
--	----------	--

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

<input checked="" type="checkbox"/>	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: Individuals grant consent by completing and submitting a patent application for processing/examination. They are notified that if a patent is granted or an application is published, the information that they submitted will become public information. Individuals must explicitly request the USPTO to transmit their information to a foreign patent office on their behalf.
<input type="checkbox"/>	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

<input checked="" type="checkbox"/>	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Individuals can submit new documents to USPTO that would replace the existing PII/BII pertaining to them.
<input type="checkbox"/>	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

<input checked="" type="checkbox"/>	All users signed a confidentiality agreement or non-disclosure agreement.
<input checked="" type="checkbox"/>	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
<input checked="" type="checkbox"/>	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
<input checked="" type="checkbox"/>	Access to the PII/BII is restricted to authorized personnel only.
<input checked="" type="checkbox"/>	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Audit Logs
<input checked="" type="checkbox"/>	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 9/17/2021 <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
<input checked="" type="checkbox"/>	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
<input checked="" type="checkbox"/>	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).

<input checked="" type="checkbox"/>	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
<input checked="" type="checkbox"/>	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
<input checked="" type="checkbox"/>	Contracts with customers establish DOC ownership rights over data including PII/BII.
<input checked="" type="checkbox"/>	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
<input checked="" type="checkbox"/>	Other (specify): All exchanged PII data are protected in accordance with NIST recommended encryption standards

- 8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

Personally Identifiable Information (PII) in TRINET is secured using appropriate administrative, physical, and technical safeguards in accordance with the applicable federal laws, executive orders, directives, policies, regulations, and standards. All access has role-based restrictions, and individuals with access privileges have undergone vetting and suitability screening. Data is maintained in areas accessible only to authorized personnel. The USPTO maintains an audit trail and performs random periodic reviews to identify unauthorized access. Additionally, TRINET is secured by various USPTO infrastructure components, including the Network and Security Infrastructure (NSI) system and other OCIO established technical controls to include password authentication at the server and database levels. All sensitive-PII at-rest and in-transit is protected in accordance with NIST recommended encryption.

Section 9: Privacy Act

- 9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

- ☒ Yes, the PII/BII is searchable by a personal identifier.
- ☐ No, the PII/BII is not searchable by a personal identifier.

- 9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

<input checked="" type="checkbox"/>	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. <i>(list all that apply):</i> PAT-TM 7 – Patent Application Forms
<input type="checkbox"/>	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
<input type="checkbox"/>	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

<input checked="" type="checkbox"/>	There is an approved record controls schedule. Provide the name of the record controls schedule: N1-241-10-1:4.2; Priority Document Exchange/Patent Examination Working Files
<input type="checkbox"/>	No, there is not an approved record controls schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
<input checked="" type="checkbox"/>	Yes, retention is monitored for compliance to the schedule.
<input type="checkbox"/>	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	<input checked="" type="checkbox"/>	Overwriting	<input checked="" type="checkbox"/>
Degaussing	<input type="checkbox"/>	Deleting	<input checked="" type="checkbox"/>
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

<input type="checkbox"/>	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
<input checked="" type="checkbox"/>	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
<input type="checkbox"/>	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact level. *(Check all that apply.)*

<input checked="" type="checkbox"/>	Identifiability	Provide explanation: General Personal Data (name, citizenship, home address, telephone number, email address) and Work-
-------------------------------------	-----------------	---

		Related Data (work address, work telephone number, work email address) can all be used to identify an individual.
<input checked="" type="checkbox"/>	Quantity of PII	Provide explanation: Quantity of PII varies depending on number of requests by applicants (PII owner) to provide this data to designated counterpart IP Offices
<input checked="" type="checkbox"/>	Data Field Sensitivity	Provide explanation: Combination of name, address, phone number, email, and citizenship may be more sensitive.
<input checked="" type="checkbox"/>	Context of Use	Provide explanation: TRINET transmits information between international patent partners. TRINET provides secure network connectivity for electronic exchange and dissemination of patent data between authenticated endpoints at the Trilateral Offices and TRINET members.
<input checked="" type="checkbox"/>	Obligation to Protect Confidentiality	Provide explanation: Applicants (PII owners) will request and designate priority application data containing PII to be provided to designated counterpart IP Offices. USPTO Privacy Policy requires the PII information collected within the system to be protected in accordance to NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information and other laws, regulations, and mandates, such as the Privacy Act of 1974.
<input checked="" type="checkbox"/>	Access to and Location of PII	Provide explanation: All access has role based restrictions, and individuals with access privileges have undergone vetting and suitability screening. Data is maintained in areas accessible only to authorized personnel. The USPTO maintains an audit trail and performs random periodic reviews to identify unauthorized access.
<input type="checkbox"/>	Other:	Provide explanation:

Section 12: Analysis

- 12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

The PII in this system poses a risk if exposed. System users undergo annual mandatory training regarding appropriate handling of information. Physical access to servers is restricted to only a few authorized individuals. The servers storing the potential PII are located in a highly sensitive zone within the cloud and logical access is segregated with network firewalls and switches through an Access Control list that limits access to only a few approved and authorized accounts. USPTO monitors, in real-time, all activities and events within the servers storing the potential PII data and personnel review audit logs received on a regular bases and alert the appropriate personnel when inappropriate or unusual activity is identified.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

<input type="checkbox"/>	Yes, the conduct of this PIA results in required business process changes. Explanation:
<input checked="" type="checkbox"/>	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

<input type="checkbox"/>	Yes, the conduct of this PIA results in required technology changes. Explanation:
<input checked="" type="checkbox"/>	No, the conduct of this PIA does not result in any required technology changes.

APPENDIX A

Warning Banner

You are accessing a U.S. Government information system, which includes: 1) this computer, 2) this computer network, 3) all Government-furnished computers connected to this network, and 4) all Government-furnished devices and storage media attached to this network or to a computer on this network. You understand and consent to the following: you may access this information system for authorized use only; unauthorized use of the system is prohibited and subject to criminal and civil penalties; you have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system at any time and for any lawful Government purpose, the Government may monitor, intercept, audit, and search and seize any communication or data transiting or stored on this information system; and any communications or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose. This information system may contain Controlled Unclassified Information (CUI) that is subject to safeguarding or dissemination controls in accordance with law, regulation, or Government-wide policy. Accessing and using this system indicate your understanding of this warning.

Points of Contact and Signatures

<p>System Owner Name: Edison Lewark Office: Infrastructure Services Division (I/ISD) Phone: (571) 272-8568 Email: Edison.Lewark@uspto.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: <u>Users, Lewark, John</u> <small>Digitally signed by Users, Lewark, John Date: 2022.09.20 16:50:19 -04'00'</small></p> <p>Date signed: _____</p>	<p>Chief Information Security Officer Name: Don Watson Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-8130 Email: Don.Watson@uspto.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: <u>Users, Watson, Don</u> <small>Digitally signed by Users, Watson, Don Date: 2022.09.26 10:24:05 -04'00'</small></p> <p>Date signed: _____</p>
<p>Privacy Act Officer Name: Caitlin Trujillo Office: Office of General Law (O/GL) Phone: (571) 270-7834 Email: Caitlin.Trujillo@uspto.gov</p> <p>I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA.</p> <p>Signature: <u>Caitlin D. Trujillo</u> <small>Digitally signed by Users, Trujillo, Caitlin Date: 2022.09.20 16:04:32 -04'00'</small></p> <p>Date signed: _____</p>	<p>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</p> <p>I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.</p> <p>Signature: <u>Users, Holcombe, Henry</u> <small>Digitally signed by Users, Holcombe, Henry Date: 2022.10.04 13:14:47 -04'00'</small></p> <p>Date signed: _____</p>
<p>Co-Authorizing Official Name: N/A Office: N/A Phone: N/A Email: N/A</p> <p>I certify that this PIA accurately reflects the representations made to me herein by the System Owner, the Chief Information Security Officer, and the Chief Privacy Officer regarding security controls in place to protect PII/BII in this PIA.</p> <p>Signature: _____</p> <p>Date signed: _____</p>	

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.