Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
Information Dissemination Support System (IDSS)

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: 2023.10.11 13:29:21 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO Information Dissemination Support System (IDSS)

Unique Project Identifier: PTOD-001-00

Introduction: System Description

Provide a brief description of the information system.

Information Dissemination Support System (IDSS) is a security boundary that includes multiple individual applications that 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. These individual applications within the IDSS boundary provide automated support for the timely search and retrieval of electronic text and images concerning patent applications, patents, trademark applications, and trademark registrations by USPTO internal and external users. IDSS itself does not search, retrieve or store any information.

Address the following elements:

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

(b) *System location*
The system location in Alexandria and Manassas, Virginia.

(c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*
IDSS interconnects with:
Service Oriented Infrastructure (SOI): SOI provides a feature-rich and stable platform upon which USPTO applications can be deployed.
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.

Trademark Processing System - Internal Systems (TPS-IS): The system includes several applications that are used to support USPTO staff through the trademark review process. TPS-IS features the ability to interface with related systems within USPTO.

Patent Capture and Application Processing System Capture - Initial Processing (PCAPS-IP): The PCAPS-IP is a Major Application (MA), 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 Capture and Application Processing System – Examination Support (PCAPS-ES): A collection of tools that facilitates USPTO examiners' ability to process, examine and review patent applications.

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

Database Services (DBS): The DBS is an Application Information System which provides a database infrastructure to support the mission of USPTO Database needs.

Patent Search System - Primary Search (PSS-PS): is a Major system, which supports the Patent Cost Center. It is considered a mission critical "system."

Trademark Next Generation (TMNG): The TMNG is a Major Application, and provides support for the automated processing of trademark applications for the USPTO.

Fee Processing Next Generation Program (FPNG): FPNG provides 21st Century Technologies and implements flexibility to quickly change business rules and other configuration changes without requiring code changes.

Trademark Processing System - External Systems (TPS-ES): The TPS-ES is a Major Application system which provides customer support for processing Trademark applications for USPTO.

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

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

(d) The way the system operates to achieve the purpose(s) identified in Section 4
IDSS implements a large, distributed and complex computing environment and each of its applications resides physically on a collection of hardware and software subsystems. IDSS uses the USPTO's network infrastructure to allow interaction between its subordinate subsystems.

(e) How information in the system is retrieved by the user
Users enter orders directly, receive the orders, and make inquiries via the internet where bulk data can also be downloaded.

(f) How information is transmitted to and from the system
Information is transmitted to and from the system via the internet.

(g) Any information sharing
IDSS conducts public information sharing through the search and retrieval of electronic texts and images concerning Patent and Trademark Applications, Patents and Trademarks by USPTO internal and external users.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information
The citation of the legal authority to collect PII and/or BII is 5 U.S.C. 301, 15 U.S.C. 1051 et seq., 35 U.S.C. 2, 35 U.S.C. 115, and E.O.12862.

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system
IDSS is considered a business-essential system with a Federal Information Processing Standard (FIPS) 199 security categorization of 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	☐	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.

☒ 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*	☐	f. Driver's License	☐	j. Financial Account	☐
b. Taxpayer ID	☐	g. Passport	☐	k. Financial Transaction	☐
c. Employer ID	☐	h. Alien Registration	☐	l. Vehicle Identifier	☐
d. Employee ID	☐	i. Credit Card	☐	m. Medical Record	☐
e. File/Case ID	☐				
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	☒	h. Date of Birth	☐	o. Financial Information	☐
b. Maiden Name	☐	i. Place of Birth	☐	p. Medical Information	☐
c. Alias	☐	j. Home Address	☒	q. Military Service	☐
d. Gender	☐	k. Telephone Number	☒	r. Criminal Record	☐
e. Age	☐	l. Email Address	☒	s. Marital Status	☐
f. Race/Ethnicity	☐	m. Education	☐	t. Mother's Maiden Name	☐
g. Citizenship	☐	n. Religion	☐		
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	☐	e. Work Email Address	☐	i. Business Associates	☐
b. Job Title	☐	f. Salary	☐	j. Proprietary or Business Information	☐
c. Work Address	☐	g. Work History	☐	k. Procurement/contracting records	☐
d. Work Telephone Number	☐	h. Employment Performance Ratings or	☐		

		other Performance Information			
l. Other work-related data (specify):					

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

System Administration/Audit Data (SAAD)					
a. User ID	☒	c. Date/Time of Access	☒	e. ID Files Accessed	☐
b. IP Address	☐	f. Queries Run	☐	f. Contents of Files	☐
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	☐	Hard Copy: Mail/Fax	☒	Online	☒
Telephone	☐	Email	☒		
Other (specify):					

Government Sources					
Within the Bureau	☒	Other DOC Bureaus	☐	Other Federal Agencies	☐
State, Local, Tribal	☐	Foreign	☐		
Other (specify):					

Non-government Sources					
Public Organizations	☐	Private Sector	☐	Commercial Data Brokers	☐
Third Party Website or Application			☐		
Other (specify):					

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

From a technical implementation, USPTO implements security and management controls to prevent the inappropriate disclosure of sensitive information. Security controls are employed to ensure information is resistant to tampering, remains confidential as necessary, and is available as intended by the agency and expected by authorized users. Management controls are utilized to prevent the inappropriate disclosure of sensitive information. In addition, the Perimeter Network (NSI) and SCS provide additional automated transmission and monitoring mechanisms to ensure that PII/BII information is protected and not breached by external entities.

2.4 Is the information covered by the Paperwork Reduction Act?

☒	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. • 0651-0009 Trademark Registrations • 0651-0032 Initial Patent Applications • 0651-0031 Patent Processing • 0651-0080 Clearance for the Collection of Qualitative Feedback on Agency Service Delivery • 0651-0078 Ombudsman Survey • 0651-0088 Improving Customer Experience (OMB Circular A-11, Section 280 Implementation)
☐	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	☐	Biometrics	☐
Caller-ID	☐	Personal Identity Verification (PIV) Cards	☐
Other (specify):			

☒	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

<u>Section 3</u>: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings	☐	Building entry readers	☐
Video surveillance	☐	Electronic purchase transactions	☐

Other (specify): Click or tap here to enter text.

☒	There are not any IT system 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	☐	For administering human resources programs	☐
For administrative matters	☒	To promote information sharing initiatives	☐
For litigation	☐	For criminal law enforcement activities	☐
For civil enforcement activities	☐	For intelligence activities	☐
To improve Federal services online	☐	For employee or customer satisfaction	☒
For web measurement and customization technologies (single-session)	☐	For web measurement and customization technologies (multi-session)	☐
Other (specify):			

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 the members of the public is used to process transactions, manage customer orders, document delivery, retrieve data, and capture documents related to the ownership of intellectual properties for both patents and trademarks. The intended use is to carry out the duties of the USPTO as outlined in 35 U.S.C. concerning the dissemination of information, and more specifically, to provide for public customer call center services. This includes tracking responses to customer requests. Data is used to ensure quality customer service for general agency information and assistance. This includes quality control purposes. In addition, the information may be used to conduct surveys of customer experience and satisfaction, and to obtain customer service recommendations.

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.)

Inadvertent private information exposure and insider threats that could impact the integrity and accessibility of the information are a risk and USPTO has policies, procedures and training to ensure that employees are aware of their responsibility of protecting sensitive information and the negative impact on the agency if there is a loss, misuse, or unauthorized access to or modification of sensitive private information. USPTO requires annual security role-based training and annual mandatory security awareness procedure training for all employees. The following are USPTO current policies; Information Security Foreign Travel Policy (OCIO-POL-6), IT Privacy Policy - (OCIO- POL-18), IT Security Education Awareness Training Policy (OCIO-POL-19), Personally Identifiable Data Removal Policy (OCIO-POL-23), USPTO Rules of the Road (OCIO-POL-36). All offices of USPTO adhere to USPTO Records Management Office's Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citation. Controls listed in 6.3 will be added here.

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	☐	☐	☒
DOC bureaus	☐	☐	☐
Federal agencies	☐	☐	☐
State, local, tribal gov't agencies	☐	☐	☐
Public	☒	☒	☐
Private sector	☐	☐	☐
Foreign governments	☐	☐	☐
Foreign entities	☐	☐	☐
Other (specify):	☐	☐	☐

☐	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?

☐	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
☒	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
☐	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.

☒	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: • Patent Capture and Application Processing System – Examination Support (PCAPSES): • NSI (Network and Security Infrastructure System) • SOI (Service Oriented Infrastructure) • ESS (Enterprise Software System) • PTO-TPS-IS - Trademark Processing System (Internal Systems) • Patent Capture and Application Processing System Capture and Initial Processing • Database Services (DBS) • PSS-PS (Patient Search System -Primary Search and Retrieval) • Trademark Next Generation (TMNG) • Trademark Processing System (External Systems) • Security and Compliance Services (SCS) • Enterprise UNIX Services (EUS) • Enterprise Windows Servers (EWS) • Fee Processing Next Generation program (FPNG) All data transmissions are encrypted and require credential verification. All data transmissions not done through dedicated lines require security certificates. Inbound transmissions as well as outbound transmissions pass through a DMZ before being sent to endpoint servers. Access controls, auditing and encryption are leveraged to prevent PII/BII leakage. In accordance with the USPTO Privacy Policy guidelines, all systems that process PII and have interconnections are designed and administered to ensure the confidentiality of PII provided to and by IDSS. Specific safeguards that are employed by the systems: • The systems and its facility are physically secured and closely monitored. Only individuals authorized by USPTO are granted logical access to the system. • Technical, operational, and management security controls are in place and are verified regularly. • Periodic security testing are conducted on the systems to help detect new security vulnerabilities on time. All personnel are trained to securely handle PII information and to understand their responsibilities for protecting PII.
☐	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	☒	Government Employees	☒
Contractors	☒		
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.)*

☒	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
☒	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	
☐	Yes, notice is provided by other means.	Specify how:
☐	No, notice is not provided.	Specify why not:

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

☒	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Information is provided on a voluntary basis. While providing this information is voluntary, if the requested information is not provided in whole or part, USPTO may not be able to complete the identity or registration process or complete it in a timely manner.
☐	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

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

☒	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: All information requested is provided on a voluntary basis.
☐	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.

☐	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how:
☒	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: There is not an external interface for customers to review/update PII/BII pertaining to them.

Section 8: Administrative and Technological Controls

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

☐	All users signed a confidentiality agreement or non-disclosure agreement.
☐	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
☒	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
☒	Access to the PII/BII is restricted to authorized personnel only.
☒	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Audit logs
☒	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): 7/28/2023 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
☒	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
☒	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).
☒	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
☒	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
☐	Contracts with customers establish DOC ownership rights over data including PII/BII.
☐	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
☐	Other (specify):

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).*

Management Controls:

a. The USPTO uses the Life Cycle review process to ensure that management controls are in place for IDSS. During the enhancement of any component, the security controls are reviewed, re-evaluated, and updated in the Security Plan. The Security Plans specifically address the management, operational and technical controls that are in place, and planned, during the operation of the enhanced system. Additional management controls include performing national agency checks on all personnel, including contractor staff.

b. The USPTO Personally Identifiable Data Extracts Policy Operational Controls:

1. Automated operational controls include securing all hardware associated with IDSS in the USPTO Data Center. The Data Center is controlled by access card entry and is manned by a uniformed guard service to restrict access to the servers, their Operating Systems and databases. Contingency planning has been prepared for the data. Backups are performed on the processing databases. Backups are stored on tape and are secured off-site. Additional operation controls include (1) Logical edit checks to ensure proper sequence of actions; (2) Physical terminal identification; (3) Database User ID; (4) Restricted data display, as required; and (5) Restricted access.

2. Manual procedures shall be followed for handling extracted data containing sensitive PII which is physically transported outside of the USPTO premises. In order to remove data extracts containing sensitive PII from USPTO premises, users must:

a. Maintain a centralized office log for extracted datasets that contain sensitive PII. This log must include the date the data was extracted and removed from the facilities, a description of the data extracted, the purpose of the extract, the expected date of disposal or return, and the actual date of return or deletion.

b. Ensure that any extract which is no longer needed is returned to USPTO premises or securely erased and that this activity is recorded on the log.

c. Obtain management concurrence in the log, if an extract aged over 90 days is still required.

d. Store all PII data extracts maintained on a USPTO laptop in the encrypted My Documents directory. This includes any sensitive PII data extracts downloaded via the USPTO Virtual Private network (VPN).

e. Encrypt and password-protect all sensitive PII data extracts maintained on a portable storage device (such as CD, memory key, flash drive, etc.). Exceptions due to technical limitations must have the approval of the Office Director and alternative protective measures must be in place prior to removal from USPTO premises.

USPTO has not developed a centralized logging system for PII data extracts. Such a system would track the following categories of information:

a. Who performed the extract,

b. When the extract was done,

c. What was the extract,

d. Where was the extract taken from,

e. Has the extract been deleted and,

f. If not deleted after 90 days, to monitor that it is still needed in 90-day intervals.

Until a system is implemented, USPTO is using the following compensating controls to protect PII data:

a. No extracts of sensitive data may be copied on to portable media without a waiver approved by the DOC CIO. The request for a waiver must include specifics as to how the data and device are protected, how long the data will be maintained, and how the data on the device will be deleted when no longer required.

b. All laptop computers allowed to store sensitive data must have full disk encryption.

c. All remote access to public USPTO systems containing sensitive data must be encrypted. A remote access to internal USPTO systems containing sensitive data must fully comply with DOC Remo Access Policy requirements.

d. All Flexi-place/telework agreements for working off-site require that adequate data protection in place.

e. Encrypt and password-protect prior to transmission any sensitive PII data extracts that are sent t an external e-mail address via the internet. The password key should be forwarded to the recipient in separate e-mail from the attached file.

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."

☒	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: COMMERCE/PAT-TM-7 Patent Application Files COMMERCE/PAT-TM-20 Customer Call Center, Assistance and Satisfaction Survey Records COMMERCE/PAT-TM-23 User Access for Web Portals and Information Requests COMMERCE/USPTO-26 Trademark Application and Registration Records
☐	Yes, a SORN has been submitted to the Department for approval on (date).
☐	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.)*

☒	There is an approved record control schedule. Provide the name of the record control schedule: N1-241-10-1:4.4 Patent Examination Feeder Records N1-241-06-2:4 Trademark Case File Feeder Records and Related Indexes N1-241-05-2:5 Information Dissemination Product Reference
☐	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
☒	Yes, retention is monitored for compliance to the schedule.
☐	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	☐	Overwriting	☐
Degaussing	☐	Deleting	☒
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.)*

☒	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
☐	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
☐	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.)*

☒	Identifiability	Provide explanation: Name, Address, Phone, Email are easily used to identify an individual.
☒	Quantity of PII	Provide explanation: The PII is publicly available and varies.
☒	Data Field Sensitivity	Provide explanation: The data includes limited personal and work-related elements and does not include sensitive identifiable information.
☒	Context of Use	Provide explanation: It provides automated support for the timely search and retrieval of electronic text and images concerning patent and trademark applications, patents and trademarks by USPTO internal and external users.
☒	Obligation to Protect Confidentiality	Provide explanation: This is done in accordance to USPTO policy (IT Security Handbook)
☒	Access to and Location of PII	Provide explanation: Due to the PII, measures are taken to ensure data is protected during processing, storage and transmission.
☐	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.)

USPTO has identified and evaluated potential threats to PII such as insider threats and adversarial entities which may cause a loss of confidentiality, accessibility and integrity of information. Based upon USPTO's threat assessment, the Agency has implemented baseline security controls to mitigate these risk to information to an acceptable level. USPTO has policies, procedures and training to ensure that employees are aware of their responsibility of protecting PII and the negative impact on the agency if there is loss, misuse, or unauthorized access to or modification of sensitive private information. USPTO requires annual security role-based training and annual mandatory security awareness procedure training for all employees.

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

☐	Yes, the conduct of this PIA results in required business process changes. Explanation:
☒	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.

☐	Yes, the conduct of this PIA results in required technology changes. Explanation:
☒	No, the conduct of this PIA does not result in any required technology changes.