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: Deborah Stephens, 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

Digitally signed by BRIAN ANDERSON
Date: 2026.03.10 06:09:27 -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 four applications, Assignment Historical Database (AHD), Assignments on the Web (AOTW), Certified Copy Center (CCC), and Patent and Trademark Assignment System (PTAS), that support the Public Records Division and Electronic Business Product Lines (EBPL). 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.

AHD – AOTW pulls information from AHD. AHD stores the information as a database.

AOTW – is a public facing application that allows users to retrieve publicly available assignment data without requiring a user to log-in.

CCC – is a patent and trademark ordering application, which allows members of the public to log-in and place an order for a patent file wrapper and other published document and trademark documents. The individuals are sent to USPTOs payment system to process the fees.

PTAS – is an internal USPTO application for processing patent and trademark assignments, which is provided to PTAS via an interconnection Intellectual Property Assignment System.

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 is located at Manassas, VA and Management Office in 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)

IDSS interconnects with:

Intellectual Property Assignment System (IPAS) – allows for electronic assignment of a patent or trademark via a website. The overall product and systems comprised of all IPAS subsystems which allows Patent and Trademark customers to request for the re-assignment of patents or trademarks via a website. Users are able to create a re-assignment request using a Trademark or Patent template, with dynamic business logic, so that all key data elements are identified and populated, attach required supporting legal documents, and make payments as necessary.

Patent Business Content Management Services (PBCMS) – Allows public users to search for patent information used during examination to make patentability determinations. The purpose of the system is to migrate current legacy services to the new cloud-based services that leverage cloud native capabilities and technologies to reduce infrastructure and operational maintenance cost to the USPTO.

First Action System for Trademarks 2 (FAST2) – FAST2 consumes data from an IDSS component. FAST2 provides the Trademark support staff with the functionality to perform actions with a more unified client interface to many disparate USPTO data sources and subsystems.

Fee Processing Next Generation (FPNG) – IDSS component retrieves fee information from FPNG and uses FPNG for payment processing. FPNG includes fee management for external customers (Financial Manager, payment page/services, and fee services consumed by other systems) and fee management for internal customers (e.g., Fee Processing Portal for processing fees and refunds).

Data Delivery System (DDS) – IDSS uses DDS component, Infrastructure Code Table (ICT), for country and state lists. The component consists of a user interface (UI) for maintaining (creating, reading, updating, deleting) reference data common to all business units as well as a collection of services making that data accessible to users and systems across the agency.

MyUSPTO Cloud (MyUSPTO-C) – IDSS uses MyUSPTO-C for user authentication. MyUSPTO-C is an external-facing web site application. It is comprised of internal and external users. The purpose of the system is to reduce the number of logins for external USPTO customers and to provide a single location from where they can conduct their business with the USPTO.

OD/BD Open Data/Big Data Master System (OD/BD MS) - OD/BD MS component, Open Data Portal (ODP), consumes data from an IDSS component. OD/BD MS is a collection of components and tools sharing analytic and data themes used in the production of business intelligence and advanced analytical solutions as well as consulting services for designing and developing those solutions.

ICAM Identity as a Service (ICAM IDaaS) – IDSS uses ICAM IDaaS for user authentication. ICAM IDaaS provides unified access management across applications and Application Programming Interface (API) based on single sign-on service. Identity and access management is provided by Okta's cloud-based solution which uses Universal Directory to create and manage users and groups.

Patent Capture and Application Processing System - Examination Support (PCAPS-ES) – IDSS uses PCAPS-ES component, One Patent Service Gateway (OPSG), for patent data validation. The purpose of PCAPS-ES is to process, transmit, and store data and images to support the data-capture and conversion requirements of the USPTO to support the USPTO patent application process.

Patent End to End (PE2E) – PE2E component, Patent Center (Patent Center), redirects users to an IDSS component so Patent Center users can place an order for patent documents seamlessly. PE2E provides examination tools for Central examination unit to track and manage the cases in this group and view documents in text format.

Patent Public Search (PPUBS) – IDSS downloads patent documents from PPUBS. PPUBS allows users to search for patent information used during examination to make patentability determinations.

Patent Trial and Appeal Case Tracking System (P-TACTS) - P-TACTS consumes data from an IDSS component. is used for electronically filing documents in connection with Inter Parties Review (IPR), Covered Business Method Patents (CBM), Post Grant Review (PGR), and Derivation Proceedings (DER) established under the Leahy-Smith America Invents Act (AIA).

Patent Business Content Management Services (PBCMS) – IDSS downloads patent documents from PBCMS component, Services - Document Wrapper for Patents (SDWP). PBCMS allows users to access patent application documents and content stored in various formats. The purpose of PBCMS is to migrate current legacy services to the new cloud-based services that leverage cloud native capabilities and technologies to reduce infrastructure and operational maintenance cost to the USPTO.

Trademark Exam (TM-EXM) - TM-EXM component, Trademark Reviewer (TM-REVIEW), consumes data from an IDSS component. TM-EXM is a center where trademark attorneys and professional staff have the ability to securely login and complete end-to-end review and processing of trademark applications/registrations.

Trademark Next Generation (TMNG) – TMNG and its various components, consumes data from IDSS. Another IDSS component also retrieves trademark documents from TSDR. TMNG is a major application that provides support for the automated processing of trademark applications for the USPTO.

Intellectual Property Leadership Management Support System (IPLMSS) –component, Trademark Trial and Appeal Board VUE (TTABVUE), consumes data from an IDSS component. IPLMSS is a major application that facilitates reporting for a range of inquiries regarding USPTO business.

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

IDSS consists of four components, AHD, AOTW, CCC, and PTAS. Each component operates differently to achieve its purpose.
AHD/AOTW – AOTW is the front-end application that allows public users to search and retrieve publicly available patent and trademark assignment information from AHD database via its Web interface. Since all information is public, users are not required to log in. AHD is a back-end database for storing publicly available patent and trademark assignment information. There is no direct user access to AHD.
CCC – CCC is a patent and trademark document ordering application that provides a public UI and an internal UI. The public UI allows public users, after logging in, to place orders for patent and/or trademark documents by using patent number, trademark number or application number. Fees for the order are processed by the USPTO payment system. The internal UI is only accessible by USPTO employees and contractors to review, process, certify and fulfill orders placed by public users.
PTAS – PTAS is an internal application that allows USPTO employees and contractors to review and process patent and trademark assignment request submitted by users from the Assignment Center application. Users can access documents in queues to advance documents in the process and finally determine whether an assignment request is recorded.

(e) How information in the system is retrieved by the user

Anyone with Public internet access can enter assignment information, receive the assignment information, and make inquiries via the Internet. USPTO internal users process assignments and orders by retrieving information through IDSS application user interface.

(f) How information is transmitted to and from the system

Information is transmitted to and from the system via the internet and the USPTO intranet.

(g) Any information sharing

IDSS through its Applications AOTW and CCC makes information available to the public. IDSS shares information to internal USPTO systems to support IDSS functionality.

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

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

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): Individuals may upload any document into IDSS to support the assignment process.					

☐ 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): Patent number, Trademark Serial Number, Assignment ID					
*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. Sex	☐	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.

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.

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.

Section 3: 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.
For USPTO internal users, IDSS uses user ID, name, work email address to authenticate users and to limit their access to IDSS application functions when performing their jobs.

For public users, IDSS uses names, home or work addresses, personal or work email address, personal or work phone numbers for processing their assignment request or orders. IP addresses and access date/time are captured in application logs as a standard practice for troubleshooting.

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 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. USPTO requires annual security role based training and annual mandatory security awareness procedure training for all employees. All offices of the USPTO adhere to the USPTO Records Management Office's Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citation.

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: IPAS PBCMS FPNG DDS MyUSPTO-C OD/BD MS ICAM IDaaS PCAPS-ES PE2E

	PPUBS P-TACTS PBCMS TM-EXM TMNG IPLMSS 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 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. USPTO requires annual security role based training and annual mandatory security awareness procedure training for all employees. All offices of the USPTO adhere to the USPTO Records Management Office's Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citation.
☐	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 the privacy policy. The privacy policy can be found at: https://www.uspto.gov/privacy-policy	
☒	Yes, notice is provided by other means.	Specify how: This PIA serves as notice.
☐	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:
☒	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: For IDSS individuals do not have an opportunity to decline to provide PII/BII to use the system and receive the services provided by the system as the information is necessary for IDSS to operate and provide its services.

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:
☒	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: Individuals do not have the opportunity to consent to particular uses of their PII/BII as it is required for the purposes of IDSS.

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: For CCC, individuals can log into their account and review and update their information. AOTW, individuals have the opportunity to review the PII as it is publicly facing but are not able to update it in AOTW. AHD, individuals have the opportunity to review the PII as it is publicly facing via the AOTW application. PTAS, USPTO employees and contractors are able to review their own information but not able to update it in PTAS.
☒	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: AOTW, individuals can not update their PII within AOTW but can reach out to USPTO customer service and they can update the individuals information on their behalf. PTAS, USPTO employees and contractors need to contact HR to update their information. Members of the public do not have an opportunity to review or update their information in PTAS as the application is not available to them. However, the individual could review and update their information through Assignment Center. AHD, individuals can access information via AOTW to review the information in AHD. Individuals can reach out to USPTO customer service to update the individuals information on their behalf.

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): 8/8/2025 ☐ 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 5 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).*

PII within the system is secured using appropriate management, operational, and technical safeguards in accordance with NIST requirements. Such management controls include a review process to ensure that management controls are in place and documented in the System Security Privacy Plan (SSPP). The SSPP specifically addresses the management, operational, and technical controls that are in place and planned during the operation of the system. Operational safeguards include restricting access to PII/BII data to a small subset of users. 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 system maintains an audit trail and the appropriate personnel is alerted when there is suspicious activity. Data is encrypted in transit and at rest.

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.)*

General Records Schedules (GRS) | National Archives

☒	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 includes all publicly available information for patents and trademarks. By statute, USPTO is required to make this information permanently available. USPTO processes thousands of these applications annually.
☒	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.)

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.

☐	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.