Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
International Data Exchange

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: 2026.04.20 18:26:23 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO International Data Exchange

Unique Project Identifier: PPL-IDE-02-00

Introduction: System Description

Provide a brief description of the information system.

International Data Exchange (IDE) is a system developed by the United States Patent and Trademark Office (USPTO) that help exchange published and unpublished application data with international stakeholders, including foreign intellectual property offices (IPOs) and the World Intellectual Property Organization (WIPO). IDE will be used by all applicants, public stakeholders, and IPOs (including examiners at the USPTO) who wish to view, monitor and exchange application data on related applications (including work sharing, priority document exchanges, and other bulk/service exchanges).

IDE is a web-based collaborative environment consisting of sub-elements:

- Cooperative Patent Classification Intellectual Property Office Collaboration Tools (CPC-IP OCT),
- Cooperative Patent Classification International (CPC INTL)
- Cooperative Patent Classification Database (CPC CDS)
- Global Dossier (GD)
- Corporative Patent Classification Database (CPC-DB)
- Sequence Listing Information Control (SLIC)
- Cooperative Patent Classification Autoclassification (CPC Autoclass)

CPC INTL and CPC-IP OCT are shared repository for all publicly available patents classification schemes approved by USPTO and the European Patent Office (EPO).

IDE sub-elements interconnect with multiple systems throughout USPTO to share patent data; including Case Management System (CMS) the central repository for patent related information, PII, and BII to make published file wrappers available to the public. The system will retrieve data from users through application programming interfaces (API's) to the interconnected systems.

CPC IP OCT is used to streamline the update, maintenance, and publication of the continuously changing Cooperative Patent Classification (CPC) Scheme & Definitions and offers the following capabilities:

- Enhanced CPC Scheme & Definitions revision project management
- Facilitate EPO and USPTO work sharing on multiple CPC revision projects
- Provide adaptive and actively maintained CPC Scheme & Definitions
- Provide common CPC Scheme & Definitions authoring tools
- Enhance bilateral collaboration via a variety of discussion tools
- Provide reporting tools for internal and international revision projects

- Generate automatically Revision Concordance List, Notice of Change (NOC), and Cross Reference List, to facilitate multiple revision projects
- Enhance CPC Classification process before and throughout the examination

CPC INTL is a web-based application hosted in USPTO Amazon Web Services (AWS) Cloud Services (UACS). CPC INTL is in a joint partnership between the USPTO and the EPO where the offices correlate their existing classification systems for a common classification scheme. CPC INTL exchanges and stores CPC classification data contained within patent documents, to be ingested from EPO and disseminated to the CPC database (CPC-DB) System through Web Services. It provides the following capabilities:

- Exchanging CPC patent classifications contained within US Patent documents with EPO.
- Retrieving CPC patent classifications contained within EPO documents.
- Ensuring that CPC patent classification data retrieved from EPO is valid and then disseminating to CPC-DB system.

CPC CDS is a web-based application that maintains and supports, Weekly Issue, Withdrawn Patent Number File (WPN), Miscellaneous Transfer Request (MTRs), Reclassification data Subclass Data file (SDF), Foreign Patent Master Classification System (FPMCF), and International Patent Classification (IPC). CPC CDS provides database information to the Bibliographic Retrieval System (BRS) and to the One Patent Service Gateway (OPSG) as up-to-date classification information. CPC CDS is used to create reference publications such as the U.S. Manual of Classification and Classification Definitions that is an ordered listing of subclasses referred to as a patent classification schedule.

GD is a web-based application that allows internal and external users to access services and view foreign IP Office published patent application dossier contents. GD provides a means to process One Portal Dossier (OPD) requests from public users via the IP5 offices, which access USPTO file wrapper content using existing USPTO OPD services. GD will provide this data to five International Intellectual Property Offices (IP5) partners (Japan Patent Office (JPO), Korean Intellectual Property Office (KIPO), EPO, China National Intellectual Property Administration (CNIPA), WIPO via services defined by international services standards that provide views of USPTO data. IP5 will use GD to share patent search examination results with public users from each office. It provides additional information on all application with the Patent Family, providing a consolidated view of the citations found in the applications so that the user can better view and utilize the cites art, and providing the dossier data in text/XML format, allowing users to download and translate or make edits to these documents.

CPC-DB provides tools to apply allocations and a master database that serves as the authoritative source for Patent Classifications placed by the USPTO, EPO and other offices.

SLIC is a processing system component for Deoxyribonucleic acid (DNA), Ribonucleic

Acid (RNA) & Protein Sequence Listings following ST.23, ST.25 and ST.26 international standards, and in accordance with 37 CFR §§ 1.821 – 1.825 "Application Disclosures Containing Nucleotide and/or Amino Acid Sequences". SLIC will intake sequence listings in ST.23, ST.25 and ST.26 formats, perform compliance verification, provide a workflow for review and data transformation for downstream intake components including Patents Content Management and Patent Search repositories. The SLIC repository is primarily for the pre-processing, post-processing and management of the sequences and their metadata. The SLIC repository is the My Structured Query Language (MySQL) database for storing metadata and will be used by SLIC exclusively.

CPC is a detailed system used to organize patent documents by technical subject so people can find related inventions more easily. Created by the USPTO and the European Patent Office, CPC divides technology into a hierarchy of sections, classes, subclasses, groups, and subgroups (for example, codes like G06F relate to computer technology). Examiners, researchers, and the public use CPC codes to search prior art, compare patents, and track developments in a technology area—making patent searching faster and more precise than relying on keywords alone.

CPC Autoclass provides an Artificial Intelligence (AI) based service to reduce/replace the current manual classification functions. Currently, the USPTO uses external contractors to manually assign classification symbols (CPC codes) to both claims and application disclosures. CPC Autoclass uses historical patent data, starting from the year 2005, stored in P-CMS (Patent Content Management System) which contains a patents' claims, abstract and specifications along with corresponding CPC codes. It then uses this knowledge to train its AI models on the relationship between CPC codes and the content of a granted patent document.

When a new patent application comes into USPTO, CPC Autoclass uses its AI models to predict what the new CPC codes will be for the new application based on the content of the application.

Address the following elements:

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

IDE is a general support system.

(b) System location

IDE cloud components are located in Amazon Web Services (AWS) US East/West cloud

IDE CPC-DB on prem component is located in Manassas, VA.

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

All of IDE system components connect to:

Patent End to End (PE2E) - Allows users to electronically file patent applications and proceedings, manage and view their in-progress patent applications and information, and view public patent applications and granted patents.

Open Data/Big Data (OD/BD) master system consists of subsystems which support the Big Data Portfolio. OD/BD resides on the UACS platform, which employs IaaS and PaaS services from AWS. The current subsystems under this master system consists of Internal Data Hub (IDH)/Data Modeling Tool (DMT), Developer Hub (DH)/Open Data Portal (ODP) and Collection of Economic Analysis Tools (COEAT)

ICAM Identity as a Service/OKTA (ICAM/IDaaS) - provides unified access management across applications and 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)- this system consist of sub-systems that process, transmit and store data and images that support the data-capture and conversion requirements of the USPTO to support the USPTO patent application process.

Data Storage Management System (DSMS): is an infrastructure system that provides archival and storage capabilities securely to the USPTO. The information system is considered an essential component of USPTO's Business Continuity and Disaster Recovery program

Cloud System Performance Monitoring (CloudSPM): provides comprehensive, real-time instrumentation and measurement that allows IT managers to optimize the performance, utilization, and availability of critical USPTO IT infrastructure, applications, platforms, including private clouds. It enables system observability and optimization for IT cloud, non-cloud, and applications**.**

Security and Compliance Services (SCS): SCS provides a centralized command and control console with integrated enterprise log management, security information and event management, network behavior analysis, and reporting through the collection of events, network/application flow data, vulnerability data, and identity information.

USPTO AWS Cloud Services (UACS): IT solutions inclusive of public cloud general support systems, scalable multi-site elastic infrastructure.

The following connect to CPC IP OCT, CPC INTL, CPC-DB, CPC CDS, and GD:

Enterprise Gateway Services (EGS) - ISD supports application-level infrastructure that provides end-point security and traffic management (load balancing) for all production USPTO applications; Maintains capabilities for Load balancing configurations for external-facing and internal applications is managed by ISD where physical management of the appliances is handled by CSB; Enhance capabilities of application-level infrastructure to provide improved operational response using existing monitoring tools and related appliances.

European Patent Office (EPO) - is one of the two organs of the European Patent Organization (EPOrg) that is responsible for administering the patent procedure and focuses on trademark and design rights in European countries.

The following connect to SLIC:

Patent Search System-Specialized Search (PSS-SS) - This system provides access to specialized data that may include annual submissions of nucleic and amino acid sequence or prior-art searching of polynucleotide and polypeptide sequences, and other types of information that may be more scientific or the technology-based, Patent Linguistic Utility Service (a query by example search system), Chemical Drawing ability, and Foreign Patent Data.

The following connect to GD and SLIC:

Patent Center (PC) – allows users to electronically file patent applications and proceedings, manage and view their in-progress patent applications and information, and view public patent applications and granted patents.

The following connect to CPC-DB:

Patent Search Artificial Intelligence (PSAI) - Patent Search AI is a platform used to provide Patent End-to-End (PE2E) Search process with AI capabilities allowing Patent Examiners to perform searches faster, identify more relevant search results. It provides CPC Suggestions: Calculates the similarity of a CPC to the topics in a document. This model provides a wider match than an exact CPC search would and is useful for finding documents with topics relevant to the provided CPC that were

missed due to high-precision instead of high-recall classification. The CPCs exactly on the document will score highly, followed by CPCs potentially missed by human classifier, then CPCs that cover topics similar to topics in the document.

The following connect to GD:

Japan Patent Office (JPO) – is a Japanese governmental agency in charge of industrial property right affairs, under the Ministry of Economy, Trade and Industry. Japan and the US have a strong cooperative relationship particularly through collaborative search programs and programs like the Patent Prosecution Highway (PPH).

Korean Intellectual Property Office (KIPO) – is the patent office and intellectual property office of South Korea. USPTO and KIPO collaborate through various programs to streamline patent prosecution and improve global IP protection. KIPO participates in the Global Patent Prosecution Highway (PPH) and the collaborative search pilot, amongst other patent protection initiatives.

World Intellectual Property Office (WIPO) – serves the world's innovators and creators, ensuring that their ideas travel safely to the market and improves lives everywhere. WIPO leads the development of a balanced and effective global intellectual property ecosystem to promote innovation and creativity for a better and more sustainable future.

China National Intellectual Property Administration (CNIPA) – is the patent and trademark office and primary intellectual property regulator of the People's Republic of China. CNIPA and USPTO collaborate through initiatives like the IP5 Patent Prosecution Highway (PPH), which allows applicants to expedite examination of patent applications if they've received a favorable decision in another participating country's office.

Patent Public Search (PPUBS) – allows public users to search for patent information used during examination to make patent ability determinations.

The following connect to CPC Autoclass:

Patent Business Content Management Services (PBCMS): The system allows users to access patent application documents and content stored in various formats.

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

IDE helps exchange published application data with international stakeholders, including foreign IPOs and the WIPO. IDE sub-elements interconnect with multiple systems throughout PTO to share patent data, including CMS (the central data repository for Patent-

related data). Users search for and request public data from the IDE sub-elements (web applications).

GD public users and web service calls access the system through the web application via the https protocol. The web application retrieves the data from interconnected USPTO systems, responds to the user request, and delivers the public data to the user via the HTTPS protocol.

CPC-DB Initial Batch Process job executes every 30 seconds to process the initial application Tar files (multiple files or subdirectories structures compressed into a single file with the extension) from RTIS, Serco and CPAglobal by calling CPC Services. In addition, the OPSG-PreExam provides CONS/DIVS initial classification Tar files. The Application Servers provide the following processing functions:

1) Receives requests from users to submit and retrieve data
2) Formats the XML messages from OPSG-PreExam, SERCO, CPA Global and RTIS for initial classification and delivers the XNL messages for OPSG-Expo to process
3) Accesses resources on other AIS applications to retrieve data

SLIC - ST.23, ST.25, and ST.26 Sequence listings enter SLIC in the Load module. SLIC loads the sequence listing with metadata into CMS repository as *.0 version. SLIC sends place.

CPC Autoclass provides CPC classification for new Patent applications. The system gathers data from the interconnected systems that are listed in interconnection section c and uses AI models to predict the CPC classification for a new application.

CPC Autoclass uses the following AI/ML models for training:

3. BERT (Bidirectional Encoder Representations from Transformers)
4. FastText

It also uses the following AI/ML models to rank the predictions output of the CPC codes by the above 2 models:

6. Logistic Regression
7. Random Forest
8. Gradient Boosting (GBM, LightGBM, CatBoost)
9. AdaBoost
10. DNN1 (Deep Neural Network 1), DNN2 (Deep Neural Network 2)

Users access the system by the web application using HTTPS protocol or by calling web services.

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

CPC-IP OCT is a web-based application that allows access by users from USPTO and EPO to view and modify Patent Classification Scheme data. USPTO uses Single Sign On (SSO) to login their users. The users are authenticated and authorized by the RBAC system which gives them the roles needed to access the application at a coarse-grained level.

CPC INTL shares this data with EPO through Web Services. There is no login needed as data is exchanged through web services using a system account.

CPC CDS and GD are web-applications that allows public users to access the system through web services. The web applications retrieve the data from interconnected USPTO systems, respond to user requests, and delivers the public data to the users.

CPC-DB has a replicated database having CPC data such as Classification Symbols, Class Definitions, Classification Schemes, and Symbol Allocations stored with USPTO and EPO. CPC DB is internal to USPTO and utilizes Single Sign on (SSO) to verify and login users.

SLIC puts the Sequence listings into the workflow. STIC reviewers can acquire the sequence listing from STIC review queue and approve/reject sequence listings as per standard process or STIC can edit the sequence listing header and create new header files but use the same body and index files from *.1 version. Editing the header creates a new version *.2 version into SLIC and get it validated by CRFValidator and attached to the workflow STIC. While SLIC creates header file for *.1 and *.2 SLIC check header information with PLAM bib data and update the header as needed.

CPC Autoclass users can access the information in the system by doing single sign on (SSO) into CPC Autoclass web application. The users are authenticated and authorized by USPTO's Okta system. Once users are authenticated, they are given access to features within the web application based on their roles. Users can search for a particular patent application and its related CPC Classifications within the web application.

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

Uses SSL/TLS 1.2/TLS 1.3 to communicate with AWS resources and information s encrypted in transit and at rest. Information is transmitted via Hyper Text Transfer Protocol Secure (HTTPS) protocol.

(g) Any information sharing

- Information is shared with foreign IP offices securely via Secure Sockets Layer (SSL) mutual TLS (HTTPS).

- The system shares published patent information with public users through a uniform resource locator (URL).

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

- 35 U.S.C §§ 382 and 383
- Leahy-Smith America Invents Act, Patent Law Treaties Implementation Act of 2021, and Patent Cooperation Treaty (PCT), which is implemented by the United States in Part IV of Title 35 of the U.S. Code (Chapters 35-37) and Subpart C of Title 37 of the Code of Federal Regulations (37 CFR 1.401-1.499), and Open Government Data Act

(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): Addition of a new component – CPC Autoclass (AI) to IDE system boundary.					

☐ 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): SLIC- File/Case ID CPC DB – Employer ID, File/Case 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): applicant name					

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.

IDE employs systems check to ensure accuracy, completeness, validity, and authenticity. Each IDE component has established specific rules or conditions for checking the syntax of information input to the system such as numbers or text, numerical ranges and acceptable values are utilized to verify that inputs match specified definitions for format and content.

The IDE 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 is controlled though role-based restrictions and individuals with privileges have undergone vetting and suitability screen. 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. The functionality of maintaining and accuracy of user accounts and respective privileges are maintained by the OKTA system which interfaces with IDE system elements.

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. 0651-0031 Initial Patent Applications 0651-0075 Hague Treaty 0651-0032 Patent Processing 0652-0021 Patent Cooperation Treaty 0651-0024 Requirements for Patent Applications Containing Nucleotide Sequence and/or Amino Acid Sequence Disclosures
☐	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).

The PII in the IDE system is in reference to USPTO employees, members of the public, contractors and foreign nationals that work for EPO (Other Federal Government Personnel). The information within the system promotes information sharing initiatives, improves federal services online and helps improve administrative matters by retrieving information from Content Management System (CMS- the central data repository for Patent-related data) and the interconnected systems within PTO to provide data to the public including international IP offices, WIPO and foreign nationals.

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.)

The threats to the system are foreign adversaries, insider threats and adversarial entities. In the event of a 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 that 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.

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 ICAM-IDaaS PE2E PCAPS-ES EGS PSS-SS PC PPUBS PSAI OD/BD DSMS CloudSPM SCS UACS EPO JPO KIPO WIPO CNIPA PBCMS 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 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: 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: Applicants are required to provide respective PII/BII to submit a patent application. A patent application is not considered complete if the PII/BII required is missing.

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: Applicants are provided the opportunity to decline to have their patent information published. (PTO/SB/35 Request for Non-Publication form.) Individuals who apply have the ability to decline to provide PII/BII by not submitting their information for application retrieval and access.
☐	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: Individuals do not have the opportunity to review/update their PII/BII within the system. For CPC INTL, CPC IP-OCT, CPC-DB, CPC-CDS, CPC Autoclass users would need to contact the admin of the source System to change the information. For SLIC and GD individuals have the opportunity to review/update PII/BII pertaining to them by contacting the respective IP office and/or the USPTO to update their initial application data. The update to the initial application data will be fed to the system.

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): 10/31/2026 ☐ 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
☐	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: Nonrecord-113, Foreign Patent Documents GRS 5.1, item 020, Non-Recordkeeping Copies of Electronic Records N1-241-10-01:5.1 Patent Cooperation Treaty (PCT) Applications and Miscellaneous Records N1-241-10-1:10.1 Patent Classification Files N1-241-10-1, 05.2 Non-PCT International Files Patent prosecution-related International files that are not specific to the PCT. Temporary: Destroy when no longer needed for 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: The system uses employee identification, name, occupation, job title, work address, work telephone number, and work email address. The combination of the fields collected together can identify a particular individual.
☒	Quantity of PII	Provide explanation: The quantity to PII and/or BII in the system can vary based on the number of applications tendered. The quantity is at least in the hundreds of thousands.
☒	Data Field Sensitivity	Provide explanation: IDE contains PII/BII data that is individually traceable. The combination of the data in the fields identified in section 2.1 could together make the data fields more sensitive.
☒	Context of Use	Provide explanation: IDE helps exchange published application data with international stakeholders, including foreign IPOs and WIPO, to view, monitor and exchange application data on related applications (including work sharing, priority document exchanges, and other bulk/service exchanges).
☒	Obligation to Protect Confidentiality	Provide explanation: USPTO Privacy Policy requires the PII information collected within the system to be protected accordance to NIST SP 800- 122, Guide to Protecting the Confidentiality of Personally Identifiable Information. In accordance with the Privacy Act of 1974, PII must be protected.
☒	Access to and Location of PII	Provide explanation: The data is stored in the AWS cloud and is protected by FedRAMP privacy and security controls.
☐	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.)

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.