Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
PatentCenter (PC) System

Reviewed by: Jamie Holcombe

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

JENNIFER GOODE Digitally signed by JENNIFER GOODE
Date: 2025.06.26 13:23:33 -04'00' 6/26/2025

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO PatentCenter (PC) System

Unique Project Identifier: PPL-PC-01-00

Introduction: System Description

Provide a brief description of the information system.

PatentCenter allows Independent Inventors, registered patent attorneys/agents, and practitioner support individuals the ability to file and view patent applications electronically using a secure internet connection. Patent Center incorporates filing, retrieving and managing patent applications within a single, unified interface to ease the process of tracking patents, patent applications and follow-on documents.

Address the following elements:

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

PatentCenter is a major application.

(b) System location

Amazon Web Service (AWS) Cloud Services (UACS) East/West, Alexandria, VA.

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

PatentCenter interconnects with the following:

Information Dissemination Support System (IDSS): Includes the products and services for Patent and Trademark dissemination and assignments.

Open Data/Big Data Master System (ODBDMS): 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.

PE2E-Patent End to End (PE2E): Allows users to manage patent applications, search prior art, manage classification and make patentability determinations.

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

Fee-Processing Next Generation (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).

International Data Exchange (IDE): The system includes users' products and services that allows access to and retrieval of Patent Classifications and related work sharing events.

Identity, Credential, and Access Management - Identity-as-a-Service (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.

Intellectual Property Assignment System (IPAS): 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.

MyUSPTO Cloud (MyUSPTO-C): The webpage where external and internal users can create a uspto.gov account and start customizing a homepage specific for their profile. The new uspto.gov accounts are designed for individuals, not groups or organizations. Future updates will add the ability for organizations to share information between colleagues.

Patent Public Search (PPUBS): Allows public users to search for patent information used during examination to make patentability determinations.

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

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

PatentCenter is a web-based application with a set of tools that allow patent applicants to file, review, and manage patent applications, including a tool for accessing published prior art. Individual would navigate to PatentCenter on the uspto.gov website to file an application, the applicant will create a profile in MyUSPTO with general information and once logged-in, select

from the following options: electronic petition, new submission, existing submission or post grant. They will then follow the on-screen directions to file the application or electronic petition. To access an application, the user would navigate to PatentCenter, enter the application number and click search. The applications will be displayed for the individuals viewing or the individual may download documents associated with the application and the application itself. USPTO employees and contractors may log-in to the system to provide admin support to applicants such as correcting application issues and other general admin support to ensure the effective processing of their applications.

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

Public, published patent application data is available to all users, including unauthenticated users. Registered patent applicants are provided with unique user accounts to facilitate subsequent secure log-ins to view their submitted applications and electronic correspondence with the USPTO. Unauthenticated users may view published applications by searching by an application identifier (e.g. Application Number, Patent Number).

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

Hypertext Transfer Protocol Secure (HTTPS) is used for all data transmissions to and from the Internet, USPTO DMZ (Demilitarized Zone), and PTOnet (USPTO internal network).

(g) Any information sharing

PatentCenter receives information from patent practitioners, support staff, independent inventors and USPTO. Information is shared within the bureau and with the public when the application has the publication date and number or with an issue date and patent number.

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

35 U.S.C 1, 2, 6, 42(c), 115, 131, 184, 261
5 U.S.C 301
E.O. 9424 Establishing in the United States Patent Office a Register of Government Interests in Patents and Applications for Patents.
Leahy-Smith America Invents Act,
37 C.F.R. 1, United States Patent and Trademark Office, Department of Commerce
the Electronic Signatures in Global and National Commerce Act, Public Law 106-229;
Homeland Security Presidential Directive 12

(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):					

☐ 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): practitioner registration number and customer numbers.					
*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): Fax Number					

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.

PatentCenter employs system checks to ensure accuracy, completeness, validity, and authenticity. Each system that PatentCenter interfaces with, as listed in Section C, 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.

PatentCenter 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.

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 Patent Processing

	0651-0032 Initial Patent Processing 0651-0033 Post Allowance and Refilling 0651-0035 Representative and Address Provisions 0651-0071 Matters Related to First Inventor to File 0651-0021 Patent Cooperation Treaty 0651-0022 Deposit of Biological Materials 0651-0024 Sequence Listings 0651-0034 Secrecy and License to Export 0651-0059 Patent Petitions Related to Application and Reexaminations 0651-0073 Patent Law Treaty 0651-0075 Hague Agreement 0651-0027 Recording Assignments
☐	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): PII (correspondence information) is collected to facilitate processing and/or patent application examination submissions and issuance of U.S. patent to a patent applicant.			

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).

Patent applicant: Patent applicants, including unauthenticated users who file a patent application or representatives provide name, mailing and/or email address, and phone number to facilitate correspondence. At a minimum, information required for the processing of patent grants and pre-grant publications include name and business address.

Unauthenticated Users: USPTO does not collect any PII about these individuals when they only use PC to search and view published patents.

USPTO Contractors and Employees – IP address are logged as part of audited events. Name, work email, work phone is collected upon the creation of an account for a USPTO employee or contractor. This information is used to enable employee or contractor to communicate with customers, perform admin roles, and for the purpose of processing a patent.

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 privacy are insider threats, and foreign governments. USPTO requires annual security role-based training and annual mandatory security awareness procedure training for all employees. The annual training has made all employees aware of the possibility of insider threats and threats from adversarial or foreign entities and how these bad actors can affect USPTO's reputation. The following are USPTO's current policies that are adhered to: IT Privacy Policy (OCIO-POL-18), IT Security Education Awareness Training Policy (OCIO-POL-19), Personally Identifiable Data Removal Policy (OCIO-POL-23), and USPTO Rules of the Road (OCIO-POL-36). The combination of USPTO trainings and policies will help USPTO employees to recognize insider threats and threats from adversarial or foreign entities. 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.

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/BII 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 adhere to the USPTO Records Management Office's Comprehensive Records Schedule or the General Records Schedule and the corresponding disposition authorities or citations.

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: IDSS ODBDMS PE2E PBCMS FPNG IDE ICAM-IDaaS MyUSPTO-C PPUBS IPAS 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 also serves as a 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: Individuals do not have the opportunity to decline to provide PII/BII. For filing, PII/BII is required to process an application. By declining to provide PII/BII the individual would not be able to apply for processing. Government individuals do not have the opportunity to decline to provide PII/BII as it is necessary for the work to be performed. For retrieval, PII/BII is not required or collected.

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: The individual does not have the opportunity to consent to a particular use of their PII/BII as the information is only collected and used for the purpose the individual is submitting the information.

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: Individuals can review and update their information directly in PatentCenter via the corrected Application Data Sheet (ADS) and customer number management.
☒	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: For USPTO employees and contractors are able to review the information in Patent Center but, they would need to reach out to HR for amendments.

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: By reviewing 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): ☒ 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 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): All sensitive-PII at-rest and in-transit are protected in accordance with NIST recommended encryption.

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).*

Adversarial entities, foreign governments, insider threats and inadvertent private information exposure are all risks 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 current USPTO policies; Information Security Foreign Travel Policy (OCIO-POL-6), IT Privacy Policy (OCIOPOL-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 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. 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 authorize personnel. The USPTO maintains an audit trail and performs random periodic reviews to identify unauthorized access. Additionally, PatentCenter is secured by various USPTO infrastructure components and other OCIO established technical controls to include password authentication at the server and database levels. All PII at-rest and in-transit is protected in accordance with NIST recommended encryption.

Section 9: Privacy Act

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

☒ Yes, the PII/BII is searchable by a personal identifier.

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

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

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

☒	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: Patent Application Files-COMMERCE/PAT-TM-7 Patent Assignment Records-COMMERCE/PAT-TM-9 Petitioners for License to File for Foreign Patents-COMMERCE/PAT–TM–13 Access Control and Identity Management System-COMMERCE/DEPT 25 Employee Personnel Files Not Covered by Notices of Other Agencies-COMMERCE/DEPT-18 USPTO PKI Registration and Maintenance System COMMERCE/PAT-TM-16 USPTO Identification and Security Access Control System COMMERCE/PAT-TM-18
☐	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: Evidentiary Patent Applications N1-241-10-1:4.1 Patent Examination Working Files N1-241-10-1:4.2 Patent Examination Feeder Records N1-241-10-1:4.4 GRS 5.1, item 020, Non-Recordkeeping Copies of Electronic Records Patent Case Files, Granted N1-241-10-1:2
☐	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 PII/BII captured by PatentCenter specifically identifies patent applicants/businesses - name, mailing address, phone number and email addresses.
☒	Quantity of PII	Provide explanation: Approximately 100k rows of data received per year associated with the applications.
☒	Data Field Sensitivity	Provide explanation: PII/BII (Intellectual Property) stored in the system is data collected from USTPO employees, contractor personnel and patent applicants in which the information is confidential and unique to those individuals. Any unauthorized access, modification, and/or disclosure of sensitive data would have a Moderate impact on the organization and its operations.
☒	Context of Use	Provide explanation: The data captured, stored, or transmitted by the PatentCenter system is used to process patent applications and may include sensitive information from the applicant's application correspondence. The data traversing PatentCenter and interconnected systems mentioned above facilitate patent application prosecution and may include non-sensitive information (i.e., applicant/examiner correspondence info
☒	Obligation to Protect Confidentiality	Provide explanation: USPTO examiners are obligated to protect applicant's identity and Intellectual Property while patent application is undergoing patent prosecution.
☒	Access to and Location of PII	Provide explanation: The information captured, stored, and transmitted by the PatentCenter system is accessed within USPTO AWS Cloud Services
☐	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.)

Nation states, adversarial entities, and insider threats are the predominant threats to the information collected and its privacy. Security controls following FedRAMP and NIST guidance were implemented to deter and prevent threats to privacy. USPTO has identified and evaluated potential threats to PII such as loss of confidentiality and integrity of information. Based upon USPTO's threat assessment policies, procedures, and training has been implemented to ensure that employees are aware of their responsibility to protect PII and to be aware of insider threats. Our employees are aware of the negative impact to the agency if there is a loss, misuse, or unauthorized access to or modification of PII.

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.