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

Privacy Impact Assessment
for the
Patent Search AI (PSAI)

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

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

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

Users, Holcombe, Henry

Digitally signed by Users, Holcombe, Henry
Date: 2023.09.06 13:05:06 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment USPTO Patent Search AI (PSAI)

Unique Project Identifier: PTOC-00-060-00

<u>Introduction</u>: System Description

Provide a brief description of the information system.

Patent End to End (PE2E) is a new web-based system that integrates all phases of the patent application process into a unified set of tools that can be accessed through a single user interface.

Search, one of the primary components of PE2E is the application used by examiners to search prior art documentation to make patentability decisions. Due to exponential growth in patents submissions over the years, Patent Examiners have experienced challenges using traditional search tools to efficiently and effectively find the 'right' references to enable them make appropriate patentability decisions. To address this challenge, USPTO decided to leverage emerging technology and implemented an Artificial Intelligence (AI) solution to augment its current search systems to help the agency's 9,000+ examiners perform search faster, identify more relevant results, deliver better and more thorough output.

Patent Search Artificial Intelligence (PSAI) is the system of choice designed to address the challenges describe above. It combines AI Technologies that are specifically custom-made machine learning (ML) models, cloud-based deployments and user experience development integrated with PE2E Search. The intended purpose of the PSAI system (with AI capabilities) is to augment existing PE2E search user interface in a manner that allows examiners to perform searches faster, identify more relevant search results, deliver better and more thorough output in a high compute and secure cloud environment hosted in Google Cloud Platform (GCP).

A component of the PSAI search experience is the 'Similarity Search' feature that leverages AI Capabilities to provide examiners with similar results based on application data to inform search strategies and identify relevant prior art. Similarity Search will be delivered as a new gadget within the existing PE2E System and will utilize similar patterns and show users patent application and document data accordingly. The gadget operates within an iFrame and will integrate directly with PE2E features within a workspace.

Address the following elements:

(a) *Whether it is a general support system, major application, or other type of system*
Patent Search AI is a Minor Application.

(b) *System location*

The system lives in two places. The end users of the application use the Gadget which operates within an iFrames and integrates directly with PE2E features within a workspace. The backend of the system resides in the USPTO's private Google Cloud environment (Google Cloud Platform us-east4 region) and deployed across three different availability zones (us-east4-a, us-east4-b and us-east4-c).

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

Patent End to End (PE2E) – PE2E serves all of Patents and is composed of 3 components, PE2E-OC, PE2E-DAV, and PE2E-Search, and together they provide capabilities for users to review their dockets, manage their work, open applications and review contents, perform prior art searches against foreign and domestic patents and create official communications to patent applicants explaining the Office's position on patentability.

USPTO Google Cloud Services (UGCS) - a standard infrastructure platform used to support the USPTO Patent Search AI system hosted in the Google Cloud Platform (GCP) us-east4, Northern Virginia, environment.

Network and Security Infrastructure (NSI) – facilitates the communications, secure access, protective services, and network infrastructure support for all USPTO applications.

(d) *The way the system operates to achieve the purpose(s) identified in Section 4*
PSAI combines AI Technologies that are specifically custom-made machine learning (ML) models, cloud-based deployments and user experience development integrated with PE2E Search to augment existing PE2E search user interface in a manner that allows examiners to perform searches faster, identify more relevant search results, deliver better and more thorough output in a high compute and secure cloud environment hosted in Google Cloud Platform (GCP).

Outside of platform and systems architecture, PSAI leverages NOAA N Wave (Wide Area Network) WAN for network interconnections, Big Data Reservoir (BDR) Data Lake as the source for unpublished datasets pushed/transformed by Google Cloud Platform (GCP) Cloud composer to PSAI Landing zones and USPTO's CICM/SCDAD services for source code management via GitLab as well as, Continuous Integration Continuous Delivery (CICD) pipelines for collaboration with on-premises configuration components shared with other PE2E Search teams. The System is registered with all applicable enterprise system registries at USPTO, including Dynamic Operational Support Plan (DOSP) and GEARS.

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

The information in the system is retrieved by the user interface (UI) through the PE2E (via the embedded Gadget UI Search application programming interface) hosted in a USPTO secure cloud environment.

BDR extracted and transformed data through application pipeline exports using GCP Cloud Composer can be retrieved by System Admins after they have been loaded in the PSAI landing zones from BDR.

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

The information is transmitted through private encrypted network traffic between end-user (examiners) machines, PE2E Search/Gadget/Similarity Search User Interfaces, Application APIs (e.g. Search API) and the USPTO secure cloud environment. PSAI application traffic is logically protected using the USPTO PKI/signed TLS (Transport Layer Security).

BDR Patent Applications data is transmitted using Application Pipeline Export processed by GCP Cloud Composer to PSAI landing zones.

(g) Any information sharing

Published and Unpublished Patent Data will be shared within the bureau by Patent examiners and development teams on a case-by-case basis, bulk transfer, and direct access.

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

35 USC 2(b)(2), 37 CFR Part 1

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

Moderate

<u>Section 1</u>: Status of the Information System

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

☐ This is a new information system.

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

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions	☐	d. Significant Merging	☐	g. New Interagency Uses	☐
b. Anonymous to Non-Anonymous	☐	e. New Public Access	☐	h. Internal Flow or Collection	☐

c. Significant System Management Changes	□	f. Commercial Sources	□	i. Alteration in Character of Data	□
j. Other changes that create new privacy risks (specify):					

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

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

Section 2: Information in the System

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

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

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

Work-Related Data (WRD)					
a. Occupation	□	e. Work Email Address	☒	i. Business Associates	☒
b. Job Title	☒	f. Salary	□	j. Proprietary or Business Information	☒
c. Work Address	☒	g. Work History	□	k. Procurement/contracting	□

				records	
d. Work Telephone Number	☒	h. Employment Performance Ratings or other Performance Information	☐		
l. Other work-related data (specify): Examiners may place unpublished patent information, or BII, in the system which could under certain circumstances (e.g. with the Application Number and the Search Query information) identify unpublished claim infomation about an unpublished application for Patent.					

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.

Data Integrity/accuracy of information in the PSAI system is ensure through the following:

1. The system is secured using appropriate NIST 800-53 Rev5 Technical, Operational and Administrative Controls to include select NIST 800-122 Privacy Controls in accordance with the National Institute of Standards and Technology (NIST) security controls (encryption, masking, access control, auditing, configuration management, system integrity etc.).

2. Mandatory IT awareness and role-based training is required for PSAI staff who have access to the system and address how to handle, retain/store, share/disseminate, and dispose of data of all types and class.

3. The team conducts regular data validation and integration tests to include Application unit tests that provide validation for interfaces to interact with the APIs.

4.All access has role-based restrictions and individuals with privileges have undergone vetting and suitability screening.

5.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 are deactivated and roles will be deleted from the application.

6.The team also tracks and monitor data access events across the environment to ensure changes made to data are audited and secure.

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
☐	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 IT system extracts for usage, process (ETL), maintains/stores, or disseminates PII about members of the public for patent application purposes, USPTO employees and contractors. The PII/BII data is collected through end-user interactions that provide click data about the actionable requests within the system's UI. The PII collected by the system is used to monitor trends in system use and used to identify individuals that have interacted with the system in a defined date and/or time range. Bulk data retrieved from the system is analyzed to determine usage by end users/system functionality. Employee satisfaction is improved since the system is designed to assist patent examiners during their work flow by providing the capability to perform faster searches and the ability to identify search results that are more relevant to their current work.

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 potential threat lies in the exposure of BII, specifically unpublished patent information. The BII that will be placed in the system could, under certain circumstances (e.g. with the Application Number and the Search Query information) identify unpublished claim information about an unpublished application for Patent. Insider threats and adversarial entities are also threats to privacy, they may cause a loss of confidentiality and integrity. PII/BII is handled such that all contractors with access to the information are under NDAs, and government personnel interacting with the data are trained regarding PII/BII privacy concerns (e.g. most government personnel are former patent examiners who directly handled the BII and are familiar with the relevant laws, rules, and regulations around the handing of such data).

<u>Section 6</u>: 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: PE2E 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 adhere to the USPTO Records Management Office's Comprehensive Records Schedule or the General Records Schedule and the corresponding disposition authorities or citations.
□	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

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

Class of Users			
General Public	□	Government Employees	☒

Contractors	☒		
Other (specify):			

Section 7: Notice and Consent

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

☒	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
☒	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://www.uspto.gov/privacy-policy	
☐	Yes, notice is provided by other means.	Specify how:
☐	No, notice is not provided.	Specify why not:

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

☐	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
☒	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: Individuals do not have the ability to decline to provide PII/BII since the information is needed to process their patent application data in the originating systems. Data is used to improve IT systems and is collected in a manner that does not allow for selective PII/BII collection.

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: Patent applicants do not have the opportunity to consent to particular uses of their information, as USPTO is required to collect and process the PII/BII, in order to process patent applications. If the patent applicant, does not consent, they cannot file a patent. Patent applications are required by law to have the inventor's information including name. Data is used to improve IT systems and is collected in a manner that does not allow for selective PII/BII usage. Employees that have their PII within this system have the opportunity to update their information within other systems.

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: Patent applicants have the opportunity to review/update their information within the originating system. Data is used to improve IT systems and is collected in a manner that does not allow for selective PII/BII changes. Patent applications are required by law to have the inventor's information including name. Employees that have their PII within this system have the opportunity to update their information within other systems.

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: PSAI system monitors and logs all data and events for security analysis.
☒	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): 4/25/2023 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
☒	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
☒	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
☒	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
☒	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
☒	Contracts with customers establish DOC ownership rights over data including PII/BII.
☐	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
☐	Other (specify):

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

Administrative Controls

Governance Risk and Compliance
PSAI leverages 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, Technical, Management, Privacy and HVA controls that are in place and planned during the operation of the system.

NDAs, IT Training and Awareness
PII/BII is handled such that all contractors with access to the information are under NDAs, and government personnel interacting with the data are trained regarding PII/BII privacy concerns (e.g. most government personnel are former patent examiners who directly handled the BII and are familiar with the relevant laws, rules, and regulations around the handing of such data). Also, system users undergo annual mandatory training regarding appropriate handling of infomation.

Technical and Operational Controls

Access Control, Audit and Account Review

PSAI will leverage Okta for enterprise identity management using OIDC to secure access to user-owned assets within GCP.

PSAI is designed to restrict access to PII/BII data to users on a need-to-know basis and all access has role-based restrictions and individuals with access privileges have undergone extensive agency background checks. Data is maintained in areas accessible only to authorized personnel.

Access to individual's PII is controlled through the application, and all personnel who access the data must first identify and authenticate with agency provided/unique credentials to the system at which time an audit trail is generated and retained indicating time of access and type of activity.

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 are deactivated and roles will be deleted from the application.

Encryption and Other Cryptographic Protections.
Data pushed from the BDR system to the Landing zone for ETL processing is encrypted through Agency managed PKI Certificate. The data is also encrypted at rest in storage buckets by using Google managed AES-256 encryption.

PSAI application traffic from on-premise to cloud is logically protected using the USPTO PKI / signed TLS 1.2 (Transport Layer Security) in the GCP load balancers for networked traffic into the application subnets.

PSAI monitors and prevents change error of PKI certificates with regards to network traffic for applications behind the configured load balancers with the following standard processes:

- The PKI certificates are encrypted and versioned through the standard USPTO version control system, GitLab.
- The load balancers and domains for each PKI certificate is managed in Infrastructure as Code configurations using Terraform.
- Any changes to PSAI infrastructure as code modules, or configurations, requires review and approval.
- This will notify of any changes that have been made to the encrypted PKI certificates.
- If configurations and changes are approved, only then, PSAI operations engineers are able to apply changes to the load balancers that are configured with the PKI certificates.

The system maintains an audit trail and the appropriate personnel is alerted when there is suspicious activity.

Incident and Event Monitoring
PSAI System uses the Agency's C3 QRadar and its internal tools such as GCP monitoring and Grafana to monitor and track events across the environment to ensure changes made to data are audited.

System Integrity Protections
The system leverages USPTO DevSecOps Change Management Policy and Procedures to drive its secured infrastructure build, code base and configuration management culture while leveraging secured open-source tools within the DevSecOps CICD Pipeline such as Chekov, Owasp Zap, Drift and other integrity check tools.

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)*: PAT-TM 7: Patent Application Files (Note: This notice is broken down, where indicated, into three subsystems relating to the status of the files: a. Pending; b. Abandoned; and c. Patented.). COMMERCE/DEPT-25: Access Control and Identity Management System
☐	Yes, a SORN has been submitted to the Department for approval on (date).
☐	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

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

☒	There is an approved record control schedule. Provide the name of the record control schedule:

	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 Patent Post-Examination Feeder Records N1-241-10-1:4.5 Patent Case Files, Granted N1-241-10-1:2 Abandoned Patent Applications, Not Referenced in Granted Case File N1-241-10-1:3
□	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: We are working with National Archives and Records Administration (NARA) to schedule this system. USPTO will treat the records as permanent records until they are officially scheduled otherwise.

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 combination of Name, Employee ID, and work email address can all identify a particular person.
☒	Quantity of PII	Provide explanation: The data items collected are limited to name, work email and System Administration/Audit Data and could be

		in the millions but the information is publicly available data once a patent is published.
☒	Data Field Sensitivity	Provide explanation: The combination of the data does not make the data field more sensitive.
☒	Context of Use	Provide explanation: The PII about employees and contractors are used to identify the individuals that interact with this system. The PII/BII contained in the applications reviewed with the help of the system is used in the processing of patents.
☒	Obligation to Protect Confidentiality	Provide explanation: NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M). Based on the data collected USPTO must protect the PII of each individual in accordance to the Privacy Act of 1974.
☒	Access to and Location of PII	Provide explanation: PII is located in a FIPS 199 Moderate system. The information captured, stored, and, transmitted by the PSAI system is accessible by internal USPTO users. Due to obtaining PII, necessary measures must be taken to ensure the confidentiality of information during processing, storing 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 stem from unpublished and published patents. Published information is publicly available information (e-mail addresses, names, user IDs, and Employee IDs) and poses very little risk if exposed. The correspondence related to non-published applications are made public when the application is made public (typically after a period of 18 months).

The BII that will be put into this system does not specifically identify an applicant to their application, but if compromised would release unpublished patent information. This requires that the system be FIPS 199 Moderate so that the risk of exposure is minimized.

System users undergo annual mandatory training regarding appropriate handling of information.

The servers storing the potential PII are located in a highly sensitive zone within the cloud and logical access is segregated with network/cloud Load balancers acting as firewalls 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. Insider threats and adversarial entities are also threats to privacy; they may cause a loss of confidentiality. Leadership and project teams conducted an analysis of data required in order to make the system effective and determined that the BII is required and necessary to the core functionality of the IT system. Security controls following FedRAMP and NIST guidance were implemented to deter and prevent threats to privacy. Data is protected in transit through TLS 1.2. Administrative access to the back-end is limited to trusted individuals on the development team. Access to the PSAI is controlled through RBAC enforcement. Given the limited access under this category, the threat of BII leakage is very low but can be a potential threat to privacy. Access to the user interface is not exposed to the public internet and only kept internally within the USPTO network.

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.

Points of Contact and Signatures

System Owner

Name: Jonathan Horner
Office: Office of Information Technology for Patents (P/OITP)
Phone: (571) 270-7358
Email: Jonathan.Horner@uspto.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: Users, Horner, Jonathan R. Digitally signed by Users, Horner, Jonathan R. Date: 2023.08.29 08:57:19 -04'00'

Date signed: ______________________________

Chief Information Security Officer

Name: Timothy S. Goodwin
Office: Office of the Chief Information Officer (OCIO)
Phone: (571) 272-
Email: Timothy.Goodwin@uspto.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: Users, Goodwin, Timothy Digitally signed by Users, Goodwin, Timothy Date: 2023.09.05 17:18:13 -04'00'

Date signed: ______________________________

Privacy Act Officer

Name: Heaton John
Office: Office of General Law (O/GL)
Phone: 703-756-1240
Email: Ricou.Heaton@uspto.gov

I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA.

Signature: John Ricou Heaton Digitally signed by John Ricou Heaton Date: 2023.08.02 17:45:21 -04'00'

Date signed: ______________________________

Bureau Chief Privacy Officer and Co-Authorizing Official

Name: Henry J. Holcombe
Office: Office of the Chief Information Officer (OCIO)
Phone: (571) 272-9400
Email: Jamie.Holcombe@uspto.gov

I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.

Signature: Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry Date: 2023.09.06 13:05:43 -04'00'

Date signed: ______________________________

Co-Authorizing Official

Name: Vaishali Udupa
Office: Office of the Commissioner for Patents
Phone: (571) 272-8800
Email: Vaishali.Udupa@uspto.gov

I certify that this PIA accurately reflects the representations made to me herein by the System Owner, the Chief Information Security Officer, and the Chief Privacy Officer regarding security controls in place to protect PII/BII in this PIA.

Signature: Vaishali Udupa Digitally signed by Vaishali Udupa Date: 2023.09.11 10:39:52 -04'00'

Date signed: ______________________________

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