Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
Patent Search System – Specialized Search (PSS-SS) System

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: 2022.09.16 15:41:35 -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 System – Specialized Search (PSS-SS) System

Unique Project Identifier: PTOP-007-00

Introduction: System Description

Provide a brief description of the information system.

Patent Search System-Specialized Search (PSS-SS) is a Major Application that provides support to the Patent Cost Center. It is considered a mission critical system. PSS-SS provides access to highly 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 PSS-SS system is made up of multiple applications that allow patent examiners and applicants to effectively search the USPTO Patent data repositories.

Requests are submitted to align a bio-sequence against all available bio sequences in a system and returns the top 50 bio sequences. The system produces a listing of high-scoring alignments with an alphanumeric identifier.

The PSS-SS system is made up of the following applications that allow patents examiners and applicants to effectively search the USPTO Patent data repositories:

Automated Biotechnology Sequence Search system (ABSS)

The purpose of the ABSS system is to sustain the PTO's business function of performing prior-art searching of molecular sequences claimed in patent applications examined by Technology Center 1600 (Biotechnology). The ABSS is an in-house PTO system designed to search electronic sequence listing data submitted by applicants, and support searching of molecular sequences using data stored from both applicant submissions and public/commercial databases of published sequence information.

Catalogue Application Migration and Upgrade (CAMU)

The CAMU Application Information System (AIS) is an Information Library System used to support document tracking by the Scientific and Technical Information Center (STIC).

Electronic Chemical Drawing System (ECDS)

The primary objective of ECDS is to provide a robust chemical drawing and naming program that can be made available to Patent Business Employees as a part of the Patent Examiner's Toolkit (PET). PET is installed on the patent examiner desktop baseline.

Foreign Image and Data Load/ Foreign Image Search Capability (FIDL/FISC)

The purpose of the FIDL/FISC subsystem is to allow Production Services Branch (PSB) personnel to load foreign patent image, header, bibliographic, and classification data from tape, CD and DVD media. FIDL supports the Cooperative Patent Collaboration (CPC) Backend. The front-end search clients (EAST/WEST) retrieve all available images from FIDL.

Publication Site for Issued and Published Sequences (PSIPS)

PSIPS system is an application that provides a Web-based interface access to patent grants and publications. All PSIPS data is publicly available. The application's goal is to update the currently available repository system of Biotech Sequences, mega tables, and mega data.

Address the following elements:

(a) Whether it is a general support system, major application, or other type of system
PSS-SS is a major application information system.

(b) System location
Madison Building, 600 Dulany Street Alexandria, VA 22314

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
PSS-SS interconnects with the following:

- **PE2E (Patent End to End):** PE2E is a master system portfolio consisting of next generation Patents AIS. The goal of PE2E is to make the interaction of USPTO's users as simple and efficient as possible in order to accomplish user goals. PE2E is a single web-based examination tool providing users with a unified and robust set of tools.

- **Patent Search System Primary Search (PSS-PS):** PSS-PS is a master system that processes, transmits, and stores data and images to support the data-capture and conversion requirements of the USPTO to support the USPTO patent application process.

- **Patent Capture and Application Processing System – Examination Support (PCAPS-ES**): PCAPS-ES is a master system that provides a comprehensive prior art search capability and the retrieval of patent and related information, which comprise text and images of United States (US), European Patent Office (EPO) and Japan Patent Office (JPO patents), US pre-grant publications, Derwent data, and IBM Technical Disclosure Bulletins.

- **Patent Capture and Application Processing System – Initial Processing (PCAPS-IP):** PCAPS-IP is an AIS that provides support to the USPTO for the purposes of capturing patent applications and related metadata in electronic form; processing applications electronically; reporting patent application processing and prosecution status; and retrieving and displaying patent applications. PCAPS-IP is comprised of multiple AISes (components) that perform specific functions, including submissions,

categorization, metadata capture, and patent examiner assignment of patent applications.

- **Enterprise Desktop Platform (EDP):** EDP is an infrastructure information system that provides a standard enterprise-wide environment to manage desktops and laptops running on the Windows operating system (OS), providing United States Government Configuration Baseline (USGCB) compliant workstations.

- **Service Oriented Infrastructure (SOI):** SOI provides a feature-rich and stable platform to deploy USPTO applications.

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

- **Security and Compliance Services (SCS):** SCS provides Security Incident and Event Management, Enterprise Forensic, Enterprise Management System, Security and Defense, Enterprise Scanner, Enterprise Cybersecurity Monitoring Operations, Performance Monitoring Tools, Dynamic Operational Support Plan, and Situational Awareness and Incident Response.

- **Database Services (DBS):** DBS is an infrastructure information system that provides a Database Infrastructure to support USPTO database needs.

- **Enterprise Windows Services (EWS):** EWS is an Infrastructure information system that provides a hosting platform for major applications for USPTO.

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

- **Network and Security Infrastructure System (NSI):** The NSI is an infrastructure information system, which provides an aggregate of subsystems that facilitates the communications, secure access, protective services, and network infrastructure support for all USPTO IT applications.

- **Data Storage Management System (DSMS):** 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. DSMS consists of the following subsystems: Boyers

Data Capture System, Enterprise Tape Backup System, and Storage Infrastructure System.

(d) The way the system operates to achieve the purpose(s) identified in Section 4
The PSS-SS is an AIS that provides support to the Patent Cost Center. It is considered a mission critical "system". PSS-SS provides access to highly 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 PSS-SS system is made up of multiple applications that allow Patents examiners and applicants to effectively search the USPTO Patent data repositories.

(e) How information in the system is retrieved by the user
The user retrieves information through web interfaces connecting various sub-systems of the PSS-SS Master system.

(f) How information is transmitted to and from the system
For external connections to the DMZ, Contractor Access Zone (CAZ), and/or external networks, device management connections use SSH, PKI, and Secure ID VPN-based connections. User data connections use PKI and Secure ID VPN and SSL/TLS and only authorized USPTO systems may access the internal PTONet.

(g) Any information sharing
Data repositories allow information to be shared with internal stakeholders (e.g. technical patent examiners). Once finalized, the application information is shared with the National Center for Biotechnology Information (NCBI).

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information
USC statutory code 35 U.S.C. Section 122

(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):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

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

Work-Related Data (WRD)					
a. Occupation	☐	e. Work Email Address	☒	i. Business Associates	☐
b. Job Title	☐	f. Salary	☐	j. Proprietary or Business	☒

				Information	
c. Work Address	☒	g. Work History	☐	k. Procurement/contracting records	☐
d. Work Telephone Number	☒	h. Employment Performance Ratings or other Performance Information	☐		
l. Other work-related data (specify):					

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

System Administration/Audit Data (SAAD)					
a. User ID	☒	c. Date/Time of Access	☒	e. ID Files Accessed	☒
b. IP Address	☒	f. Queries Run	☒	f. Contents of Files	☒
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	☐	Hard Copy: Mail/Fax	☐	Online	☒
Telephone	☐	Email	☐		
Other (specify): Some bibliographic, and classification data is retrieved by personnel from tape, CD and DVD.					

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.

USPTO implements security and management controls to prevent the inappropriate disclosure of sensitive information. Security controls are employed to ensure information is resistant to tampering, remains confidential as necessary, and is available as intended by the agency and as expected by authorized users. Management controls are utilized to prevent the inappropriate disclosure of sensitive information. In addition, the Perimeter Network (NSI) and SCS provide additional automated transmission and monitoring mechanisms to ensure that PII/BII information is protected and not breached by external entities. PSS-SS employs system checks to ensure accuracy, completeness, validity, and authenticity. Each PSS-SS 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. Applicants may update their information by submitting a new application.

2.4 Is the information covered by the Paperwork Reduction Act?

☒	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. 0651-0031 Patent Processing 0651-0032 Initial Patent Application 0651-0024 Requirements for Patent Applications Containing Nucleotide Sequence and Amino Acid Sequence Disclosure
☐	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): BII is collected in order to provide comprehensive prior art search and retrieval capability to enable PTO to process patent applications.			

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).

This system contains information about members of the public, government employees, and contractors.

- PSS-SS, ABSS receives information about members of the public within the metadata from the SCORE and PSIPS applications, submitted by the public. The application submission is used for administrative matters because it is reviewed by Technical Patents Examiners as part of a patent application.

- PSS-SS, ABSS is an in-house PTO system designed to search electronic sequence listing data submitted by applicants, and support searching of molecular sequences using data stored from both applicant submissions and public/commercial databases of published sequence information, allowing government employees and contractors to share information to better perform their work remotely.

- PSS-SS data repositories promote information sharing initiatives within the bureau which allow information to be shared with internal stakeholders such as technical patent examiners.

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.)

Insider threats and foreign entities are the main threat to the system, these threats do not pose a significant risk since the information in the system becomes publicly accessible through NCBI once the patent application has been granted. USPTO has implemented NIST security controls (encryption, access control, auditing) to reduce the insider threat risk. Mandatory IT Awareness and role- based training is required for staff who have access to PSS-SS and its sub-systems. Users are taught how to handle, retain, and dispose of data properly, and reporting requirements for potential insider threat, incidents, or breaches.

NIST security controls are in place to ensure that information is handled, retained, and disposed of appropriately. For example, advanced encryption is used to secure the data both during transmission and while stored at rest. Access to individual's PII is controlled through the application and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. USPTO requires annual security role based training and annual mandatory security awareness procedure training for all employees. All offices of the USPTO adhere to the USPTO Records Management Office's Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citation.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	☒	☒	☒
DOC bureaus	☐	☐	☐
Federal agencies	☐	☒	☐
State, local, tribal gov't agencies	☐	☐	☐

Public	☐	☐	☐
Private sector	☐	☐	☐
Foreign governments	☐	☐	☐
Foreign entities	☐	☐	☐
Other (specify):	☐	☐	☐

☐	The PII/BII in the system will not be shared.

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

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

6.3 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

☒	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: PE2E PSS-PS PCAPS-ES PCAPS-IP SCS DSMS 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: See Banner Warning Appendix A.
☐	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: PSS-SS online applications (i.e. PatFT, AppFT, AIW, and PIW) facilitates public online searches of granted patents. These public tools do not require users to provide any PII/BII. The non-sensitive PII (patent owner name, correspondence address, etc.) that returns during granted patent searches are available for public record. Patent owner(s) have the opportunity to update non-sensitive PII (i.e., name, correspondence address, etc.) during and after application filing via EFS-Web and Private PAIR, respectively.

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: PSS-SS online applications (i.e. PatFT, AppFT, AIW, and PIW) facilitates public online searches of granted patents. These public tools do not require users to provide any PII/BII. The non-sensitive PII (patent owner name, correspondence address, etc.) that returns during granted patent searches are available for public record. Patent owner(s) have

		the opportunity to update non-sensitive PII (i.e., name, correspondence address, etc.) during and after application filing via EFS-Web and Private PAIR, respectively.

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: PSS-SS online applications (i.e. PatFT, AppFT, AIW, and PIW) facilitates public online searches of granted patents. Patent Owners have the opportunity to update non-sensitive PII (i.e., name, correspondence address, etc.) during and after application filing via EFS-Web and Private PAIR, respectively.
☐	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

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: The ABSS application user interface allows EIC1600 users access to view and download homology search results, some of which may contain PII/BII from biosequence listings. Tracking mechanism is possible through HTTPD logs.
☒	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 7/7/2022 ☐ 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).*

Information in USPTO information systems are protected with operational and technical controls documented in the PSS-SS System Security Plan. A Security Categorization compliant with the FIPS 199 and NIST SP 800-60 requirements was conducted for PSS-SS. The overall FIPS 199 security impact level for PSS-SS was determined to be Moderate. This categorization influences the level of effort needed to protect the information managed and transmitted by the system: • Operational controls include securing all hardware associated with the PSS-SS in the USPTO Data Center. The Data Center is controlled by access card entry and is manned by a uniformed guard service to restrict access to the servers, their operating systems, and databases. • Backups are managed by the Enterprise Tape Backup System (ETBS) and are secured off-site by First Federal. • Windows and Linux servers within PSS-SS are regularly updated with the latest security patches by the Windows and Unix System Support Groups.

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)*: USPTO PKI Registration and Maintenance System: Commerce/PAT–TM–16 USPTO Patent Application Files: Commerce/PAT-TM-7 Access Control and Identity Management System: COMMERCE/DEPT-25
☐	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: United States Patent and Trademark Office Comprehensive Records Schedule • N1-241-01-4, items d4a – f. • N1-241-10-1:5.1 • N1-241-10-1:5.2
☐	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: Name, Telephone Number, and email address can identify a particular person when combined.
☒	Quantity of PII	Provide explanation:

		The quantity of PII in the system is large enough to be concerned if disclosed.
☒	Data Field Sensitivity	Provide explanation: The combination of the data does not make the information in the system any more sensitive.
☒	Context of Use	Provide explanation: BII is not directly used by PSS-SS applications; rather it simply receives it as part of the metadata from other applications.
☒	Obligation to Protect Confidentiality	Provide explanation: The combination of the data does not make the information in the system any more sensitive. There is no obligation to protect after applications have been granted since the information becomes available to the public through NCBI portal.
☒	Access to and Location of PII	Provide explanation: The information, captured, stored, and transmitted by the PSS-SS system is maintained within USPTO systems.
☐	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.)

Adversarial entities, foreign governments, and insider threats are the predominant threats to the information collected. Security controls that conform to NIST guidance are implemented to protect the data. Inadvertent dissemination of PII/BII during the patent recall process is a risk and USPTO has policies, procedures, and training to ensure that employees are aware of their responsibility of protecting sensitive information and the negative impact to the agency if there is a loss, misuse, or unauthorized access to or modification of sensitive private information.

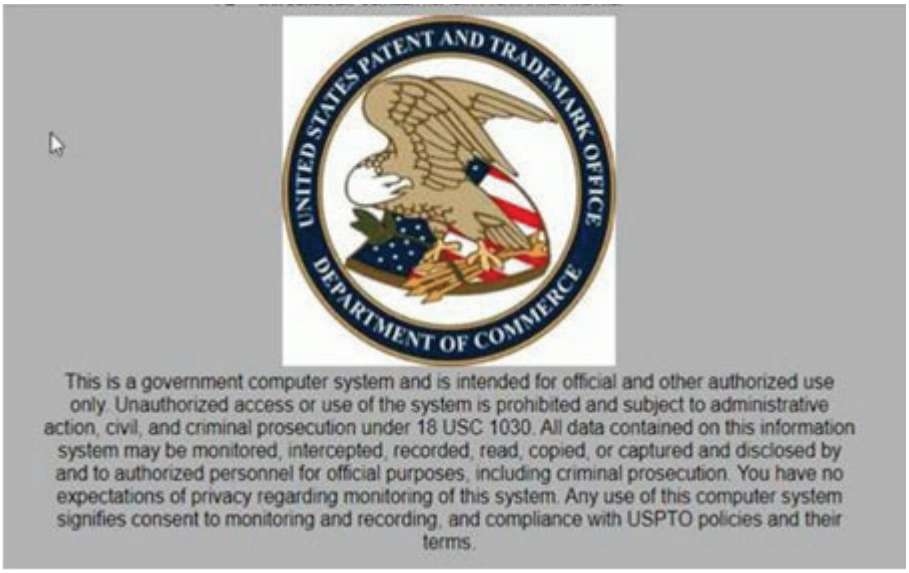
12.2 Indicate whether the conduct of this PIA results in any required business process changes.

☐	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.

Appendix A – Warning Banner



Points of Contact and Signatures

System Owner
Name: Nelson Yang
Office: Office of Patent Information Management (OPIM)
Phone: (571) 272-0826
Email: Nelson.Yang@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, Yang, Nelson Digitally signed by Users, Yang, Nelson Date: 2022.09.16 13:32:07 -04'00'

Date signed: _____

Chief Information Security Officer
Name: Don Watson
Office: Office of the Chief Information Officer (OCIO)
Phone: (571) 272-8130
Email: Don.Watson@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, Watson, Don Digitally signed by Users, Watson, Don Date: 2022.09.16 14:22:36 -04'00'

Date signed: _____

Privacy Act Officer
Name: Caitlin Trujillo
Office: Office of General Law (O/GL)
Phone: (571) 270-7834
Email: Caitlin.Trujillo@uspto.gov

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

Signature: Caitlin D. Trujillo Digitally signed by Users, Trujillo, Caitlin Date: 2022.09.15 16:25:47 -04'00'

Date signed: _____

Bureau Chief Privacy Officer and 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: 2022.09.16 15:42:04 -04'00'

Date signed: _____

Co-Authorizing Official
Name: Andrew Faile
Office: Office of the Commissioner for Patents
Phone: (571) 272-8800
Email: Andrew.Faile@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: Users, Faile, Andrew Digitally signed by Users, Faile, Andrew Date: 2022.09.19 11:14:05 -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.