

**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

JENNIFER GOODE Digitally signed by JENNIFER
GOODE
Date: 2021.09.13 17:24:20 -04'00'

09/08/2021

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)

Unique Project Identifier: PTOP-007-00

Introduction: System Description

Provide a description of the system that addresses the following elements:

The response must be written in plain language and be as comprehensive as necessary to describe the 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.

(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 2231

(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), U.S. 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.
- **Enterprise Monitoring and Security Operations (EMSO):** EMSO 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 conducted by the system

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	<input type="checkbox"/>	d. Significant Merging	<input type="checkbox"/>	g. New Interagency Uses	<input type="checkbox"/>
b. Anonymous to Non-Anonymous	<input type="checkbox"/>	e. New Public Access	<input type="checkbox"/>	h. Internal Flow or Collection	<input type="checkbox"/>
c. Significant System Management Changes	<input type="checkbox"/>	f. Commercial Sources	<input type="checkbox"/>	i. Alteration in Character of Data	<input type="checkbox"/>
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 (version 01-2015 or

01-2017).

- This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2019 or later).

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*	<input type="checkbox"/>	f. Driver's License	<input type="checkbox"/>	j. Financial Account	<input type="checkbox"/>
b. Taxpayer ID	<input type="checkbox"/>	g. Passport	<input type="checkbox"/>	k. Financial Transaction	<input type="checkbox"/>
c. Employer ID	<input type="checkbox"/>	h. Alien Registration	<input type="checkbox"/>	l. Vehicle Identifier	<input type="checkbox"/>
d. Employee ID	<input type="checkbox"/>	i. Credit Card	<input type="checkbox"/>	m. Medical Record	<input type="checkbox"/>
e. File/Case ID	<input checked="" type="checkbox"/>				
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	<input checked="" type="checkbox"/>	h. Date of Birth	<input type="checkbox"/>	o. Financial Information	<input type="checkbox"/>
b. Maiden Name	<input type="checkbox"/>	i. Place of Birth	<input type="checkbox"/>	p. Medical Information	<input type="checkbox"/>
c. Alias	<input type="checkbox"/>	j. Home Address	<input type="checkbox"/>	q. Military Service	<input type="checkbox"/>
d. Gender	<input type="checkbox"/>	k. Telephone Number	<input checked="" type="checkbox"/>	r. Criminal Record	<input type="checkbox"/>
e. Age	<input type="checkbox"/>	l. Email Address	<input checked="" type="checkbox"/>	s. Physical Characteristics	<input type="checkbox"/>
f. Race/Ethnicity	<input type="checkbox"/>	m. Education	<input type="checkbox"/>	t. Mother's Maiden Name	<input type="checkbox"/>
g. Citizenship	<input type="checkbox"/>	n. Religion	<input type="checkbox"/>		
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	<input type="checkbox"/>	e. Work Email Address	<input checked="" type="checkbox"/>	i. Business Associates	<input type="checkbox"/>
b. Job Title	<input type="checkbox"/>	f. Salary	<input type="checkbox"/>	j. Proprietary or Business Information	<input checked="" type="checkbox"/>
c. Work Address	<input checked="" type="checkbox"/>	g. Work History	<input type="checkbox"/>	k. Procurement/contracting records	<input type="checkbox"/>
d. Work Telephone Number	<input checked="" type="checkbox"/>	h. Employment Performance Ratings or other Performance Information	<input type="checkbox"/>		
l. Other work-related data (specify):					

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

System Administration/Audit Data (SAAD)					
a. UserID	<input checked="" type="checkbox"/>	c. Date/Time of Access	<input checked="" type="checkbox"/>	e. ID Files Accessed	<input checked="" type="checkbox"/>
b. IP Address	<input checked="" type="checkbox"/>	f. Queries Run	<input checked="" type="checkbox"/>	f. Contents of Files	<input checked="" type="checkbox"/>
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	<input type="checkbox"/>	Hard Copy: Mail/Fax	<input type="checkbox"/>	Online	<input checked="" type="checkbox"/>
Telephone	<input type="checkbox"/>	Email	<input type="checkbox"/>		
Other (specify):					

Government Sources					
Within the Bureau	<input type="checkbox"/>	Other DOC Bureaus	<input type="checkbox"/>	Other Federal Agencies	<input type="checkbox"/>
State, Local, Tribal	<input type="checkbox"/>	Foreign	<input type="checkbox"/>		
Other (specify):					

Non-government Sources			
Public Organizations	<input checked="" type="checkbox"/>	Private Sector	<input checked="" type="checkbox"/>
Third Party Website or Application	<input type="checkbox"/>		
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 EMSO 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 systems 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?

<input checked="" type="checkbox"/>	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
<input type="checkbox"/>	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	<input type="checkbox"/>	Biometrics	<input type="checkbox"/>
Caller-ID	<input type="checkbox"/>	Personal Identity Verification (PIV) Cards	<input type="checkbox"/>
Other (specify):			

<input checked="" type="checkbox"/>	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	<input type="checkbox"/>	Building entry readers	<input type="checkbox"/>
Video surveillance	<input type="checkbox"/>	Electronic purchase transactions	<input type="checkbox"/>
Other (specify):			
<input checked="" type="checkbox"/>	There are not any IT systems 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	<input type="checkbox"/>	For administering human resources programs	<input type="checkbox"/>
For administrative matters	<input checked="" type="checkbox"/>	To promote information sharing initiatives	<input checked="" type="checkbox"/>
For litigation	<input type="checkbox"/>	For criminal law enforcement activities	<input type="checkbox"/>
For civil enforcement activities	<input type="checkbox"/>	For intelligence activities	<input type="checkbox"/>
To improve Federal services online	<input checked="" type="checkbox"/>	For employee or customer satisfaction	<input type="checkbox"/>
For web measurement and customization technologies (single-session)	<input type="checkbox"/>	For web measurement and customization technologies (multi-session)	<input type="checkbox"/>
Other (specify): BII data is submitted by Scientists. To provide a comprehensive prior art search capability and the retrieval of patent and related information for dissemination to the public based on requirements stated in USC statutory code 35 U.S.C Section 122.			

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).

<p>This system contains information about members of the public, government employees, and contractors.</p> <ul style="list-style-type: none"> • 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.

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	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DOC bureaus	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Federal agencies	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
State, local, tribal gov't agencies	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Private sector	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign governments	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign entities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other (specify):	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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?

<input type="checkbox"/>	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
<input checked="" type="checkbox"/>	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
<input type="checkbox"/>	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.

<input checked="" type="checkbox"/>	<p>Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII.</p> <p>Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>System Name</th> <th>Organization</th> </tr> </thead> <tbody> <tr> <td>PCAPS-ES</td> <td>USPTO</td> </tr> <tr> <td>PCAPS-IP</td> <td>USPTO</td> </tr> <tr> <td>PE2E</td> <td>USPTO</td> </tr> </tbody> </table> <p>By restricting access to the system via Active Directory, PSS-SS and PSS-PS' protection of BII and PII data is performed by the implemented AD automated system. Automatic quality control for data checks exist. VPN is used for developer access. There is a network connection to the Internet via the Network Perimeter for PSS-SS and PSS-PS users. The PSS-SS and PSS-PS services are logically partitioned via a DMZ and an internal USPTO firewall is used as the boundary protection device that secures the communication between Internet users and the PSS-SS and PSS-PS. This connection is protected and</p>	System Name	Organization	PCAPS-ES	USPTO	PCAPS-IP	USPTO	PE2E	USPTO
System Name	Organization								
PCAPS-ES	USPTO								
PCAPS-IP	USPTO								
PE2E	USPTO								

	controlled by the USPTO infrastructure.
<input type="checkbox"/>	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	<input type="checkbox"/>	Government Employees	<input checked="" type="checkbox"/>
Contractors	<input checked="" type="checkbox"/>		
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.)*

<input checked="" type="checkbox"/>	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
<input checked="" type="checkbox"/>	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: See Banner Warning Appendix A	
<input type="checkbox"/>	Yes, notice is provided by other means.	Specify how:
<input type="checkbox"/>	No, notice is not provided.	Specify why not:

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

<input type="checkbox"/>	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
<input checked="" type="checkbox"/>	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.

<input type="checkbox"/>	Yes, individuals have an opportunity to consent to particular uses of their	Specify how:
--------------------------	---	--------------

	PII/BII.	
<input checked="" type="checkbox"/>	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.

<input type="checkbox"/>	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how:
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	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.

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. (Check all that apply.)

<input checked="" type="checkbox"/>	All users signed a confidentiality agreement or non-disclosure agreement.
<input checked="" type="checkbox"/>	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
<input checked="" type="checkbox"/>	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
<input checked="" type="checkbox"/>	Access to the PII/BII is restricted to authorized personnel only.
<input checked="" type="checkbox"/>	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.
<input checked="" type="checkbox"/>	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): <u>07/01/2021</u> <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
<input checked="" type="checkbox"/>	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
<input checked="" type="checkbox"/>	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).

<input checked="" type="checkbox"/>	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
<input checked="" type="checkbox"/>	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
<input type="checkbox"/>	Contracts with customers establish DOC ownership rights over data including PII/BII.
<input type="checkbox"/>	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
<input type="checkbox"/>	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.”

<input checked="" type="checkbox"/>	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. <i>(list all that apply):</i> 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
<input type="checkbox"/>	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
<input type="checkbox"/>	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.)*

<input checked="" type="checkbox"/>	There is an approved record controls schedule. Provide the name of the record controls schedule: United States Patent and Trademark Office Comprehensive Records Schedule FY2018
-------------------------------------	---

<input type="checkbox"/>	No, there is not an approved record controls schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
<input checked="" type="checkbox"/>	Yes, retention is monitored for compliance to the schedule.
<input type="checkbox"/>	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	<input type="checkbox"/>	Overwriting	<input checked="" type="checkbox"/>
Degaussing	<input type="checkbox"/>	Deleting	<input checked="" type="checkbox"/>
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.)

<input type="checkbox"/>	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
<input checked="" type="checkbox"/>	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
<input type="checkbox"/>	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.)

<input checked="" type="checkbox"/>	Identifiability	Provide explanation: Name, Telephone Number, and email address can identify a particular person when combined.
<input checked="" type="checkbox"/>	Quantity of PII	Provide explanation: The quantity of PII in the system is large enough to be concerned if disclosed.
<input checked="" type="checkbox"/>	Data Field Sensitivity	Provide explanation: The combination of the data does not make the information in the system any more sensitive.
<input checked="" type="checkbox"/>	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.
<input checked="" type="checkbox"/>	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.
<input checked="" type="checkbox"/>	Access to and Location of PII	Provide explanation: The information, captured, stored, and transmitted by the PSS-SS system is maintained within USPTO systems.
<input type="checkbox"/>	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.

<input type="checkbox"/>	Yes, the conduct of this PIA results in required business process changes. Explanation:
<input checked="" type="checkbox"/>	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.

<input type="checkbox"/>	Yes, the conduct of this PIA results in required technology changes. Explanation:
<input checked="" type="checkbox"/>	No, the conduct of this PIA does not result in any required technology changes.

Appendix A – Banner Warning



This is a government computer system and is intended for official and other authorized use only. Unauthorized access or use of the system is prohibited and subject to administrative action, civil, and criminal prosecution under 18 USC 1030. All data contained on this information system may be monitored, intercepted, recorded, read, copied, or captured and disclosed by and to authorized personnel for official purposes, including criminal prosecution. You have no expectations of privacy regarding monitoring of this system. Any use of this computer system signifies consent to monitoring and recording, and compliance with USPTO policies and their terms.

[FM: Systems Privacy Policy](#)