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: Deborah Stephens, Bureau Chief Privacy Officer

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

Digitally signed by BRIAN ANDERSON
Date: 2025.10.29 13:22:20 -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 General Support System (GSS) that provides access to specialized data that may include annual submissions of nucleic and amino acid sequence or prior-art searching of polynucleotide and polypeptide sequences, and other types of information that may be more scientific or the technology-based, Patent Linguistic Utility Service (a query by example search system), Chemical Drawing ability, and Foreign Patent Data. The PSS-SS system is made up of three applications that allow patent examiners and applicants to effectively search the United States Patent and Trademark Office (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 patent 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 USPTO 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.

Electronic Chemical Drawing System (ECDS)
ECDS is a Commercial-off-the-shelf (COTS) product installed on employee workstations. 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.

Publication Site for Issued and Published Sequences (PSIPS)
The Publication Site for Issued and Published Sequences (PSIPS) is a cloud-based application that provides a web-based interface allowing external users access to patent grants and publications. PSIPS acts as a storage and retrieval site for bio-sequence listings that are at least 300 pages (roughly 600Kb), mega table sections that are at least 200 contiguous pages, and other mega items. This data has been included in either a granted US patent or a published US

patent application. Using PSIPS, users can view or download individual sequences or tables, or download the entire bio-sequence Listing, mega table section, or other mega table items.

Address the following elements:

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

PSS-SS is a GSS.

(b) System location

ABSS and ECDS system is located in Manassas, VA .

PSIPS system is located in the Amazon Web Services (AWS) US East/West cloud, Alexandria, VA.

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

PSS-SS and its components interconnect with

ICAM Identity as a Service (ICAM-IDaaS) - provides unified access management across applications and APIs based on single sign-on service. Identity access management is provided by Okta's cloud-based solution which uses Universal Directory to create and manage users and groups.

Enterprise Software Services (ESS) - is comprised of multiple on premise and in-the-cloud software services, which support the USPTO in carrying out its daily tasks. Within this system, the services are broken up into several subsystems (Enterprise Active Directory Services (EDS), MyUSPTO, Role-Based Access Control (RBAC), Email as a Service (EaaS), Enterprise Share Point Services (ESPS), Symantec Endpoint Protection, and Patent Trademark Office Fax (PTOFAX).

Enterprise Windows Servers (EWS) - is an information system that provides a hosting platform to support various USPTO missions to safeguard memory on hardware and software through Data Execution Prevention (DEP).

Network and Security Infrastructure System (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) - 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.

Security and Compliance Services (SCS) - is a general support system comprised of subsystems which work together to provide enterprise level monitoring to the USPTO.

International Data Exchange (IDE) – ABSS connects to the subcomponent Sequence Listing Information Control (SLIC) of IDE. It is a system component for Deoxyribonucleic acid (DNA), Ribonucleic acid (RNA) & Protein Sequence Listings following ST.23, ST.25, and ST.26 international standards, and in accordance with 37 CFR §§ 1.821 – 1.825 "Application Disclosures Containing Nucleotide and/or Amino Acid Sequences". SLIC will intake sequence listings in ST.23, ST.25 and ST.26 formats, perform compliance verification, provide a workflow for review and data transformation for downstream intake components including Patents Content Management and Patent Search repositories. The SLIC repository is primarily for the pre-processing, post-processing and management of the sequences and their metadata.

Patent Administrative Center (PAC) – provides central tracking and recording of patent application status and bibliographic data; and its components will directly support the administration of the application processing lifecycle by facilitating the scanning of application documents, initialization of new patent applications, review of security, formality, document & fee requirements; automated routing of applications; generation, review and mailing of official correspondence to applicants; tracking examiner productivity; and the publication and issuing of patents.

Patent Capture and Application Processing System – Examination Support (PCAPS-ES) – ABSS interconnects with the component Service- One Open Service Gateway(S-OPSG) from PCAPS-ES. It is a product component that supports the Patent Administrative Center product under the Patent Product Line. OPSG serves as the owner and manager of patent application information, including the development, operations and maintenance of database assets known as Patent Application Locating and Monitoring (PALM). Users can not directly consume the OPSG, it supports the Patent Corps and Agency end user community via the Patent Data Portal, allowing users to search for patent application information and status throughout the entire prosecution life cycle.

Patent End to End (PE2E) – is a Master system portfolio consisting of next generation Patents Automatic Identification System (AIS).

Patent Business Content Management Services (PBCMS) – ABSS connects to the PBCMS component Services – Document Wrapper for Patents(S-DWP). This service supports retrieval/load of Patent Application data to a centralized Content Management System (CMS). The Restful services provided by S-DWP are used by Internal USPTO Patent components to access patent images and metadata. Additionally, this service provides user/team management, application/document management, & messaging services for PE2E Docket and Application Viewer (DAV). The component provides centralized document access, high availability and improved performance through the use of Representational State Transfer (REST) services.

Reed Tech Patent Data and Document Management System (Reed Tech PDDM) – is a publisher for patent applications.

The PSS-SS component ECDS has no interconnections with USPTO systems. ECDS is a ChemDraw COTS software to the employee workstations, the creation of a shortcut in the Patent Examiner's Toolkit or on the desktop as part of the installation package and the creation of a ChemDraw folder on the user's workstation that is designated as the default for saving chemical drawing files.

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

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

Information is encrypted in transit via Hyper Text Transfer Protocol Secure (HTTPS) protocol.

(g) Any information sharing

- Data repositories allow information to be shared with internal stakeholders (e.g., technical patent examiners).

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

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

USC statutory code 35 U.S.C. Section 122, 5 USC 301, 35 USC 2 and 115

(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): UserID – PSIPS internal module, external module does not collect information Application ID - ABSS					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

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

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

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

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

Other Information (specify)

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

Directly from Individual about Whom the Information Pertains					
In Person	☐	Hard Copy: Mail/Fax	☐	Online	☒
Telephone	☐	Email	☐		
Other (specify):					

Government Sources					
Within the Bureau	☒	Other DOC Bureaus	☐	Other Federal Agencies	☐
State, Local, Tribal	☐	Foreign	☐		
Other (specify):					

Non-government Sources					
Public Organizations	☒	Private Sector	☐	Commercial Data Brokers	☐
Third Party Website or Application			☐		
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

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 parent 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).

- PSS-SS, ABSS receives information about members of the public within the metadata from the SLIC 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 USPTO 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, DOC employees, and contractor.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

The threats to the system are foreign adversaries, insider threats and adversarial entities. In the event of computer failure, insider threats, or attack against the system by adversarial or foreign entities, any potential PII data stored within the system could be exposed. To avoid a breach, the system has certain security controls in place to ensure the information is handled, retained, and disposed of appropriately. Access to individual's PII is controlled through the application, and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. These audit trails are based on application server out-of-the-box logging reports reviewed by the Information System Security Officer (ISSO) and System Auditor and any suspicious indicators such as browsing will be immediately investigated and appropriate action taken. Also, system users undergo annual mandatory training regarding appropriate handling of information.

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: PBCMS IDE PE2E PCAPS-ES ICAM-IDaaS ESS DSMS PAC ReedTech PDDM 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: PSIPS web-interface facilitates public online searches of granted patents and publications. This public tool does 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. ABSS is an internal system that inherits the PII/BII constraints from Patent Center and SLIC that feed biosequence data to ABSS, therefore the individuals do not have an opportunity to decline to provide PII/BII.

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: PSIPS web-interface facilitates public online searches of granted patents and publications. This public tool does 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. ABSS is an internal system that inherits the PII/BII constraints from Patent Center and SLIC that feed biosequence data to ABSS. Therefore, PSS-SS does not provide individuals opportunity to consent to particular uses of their PII/BII.

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: PSS-SS: PSIPS web-interface facilitates public online searches of granted patents and publications. This public tool does 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. ABSS is an internal system that inherits the PII/BII constraints from Patent Center and SLIC that feed biosequence data to ABSS. Therefore, though individuals may review the PII/BII that is available via the public record they would not be able to make the updates within the system and would need to contact USPTO.

Section 8: Administrative and Technological Controls

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

☒	All users signed a confidentiality agreement or non-disclosure agreement.

☒	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
☒	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
☒	Access to the PII/BII is restricted to authorized personnel only.
☒	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Audit logs events are being captured, monitored, and tracked through SIEM QRADAR. In addition, audit logs are captured and monitored through AWS cloud services.
☒	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): 6/12/2025 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
☒	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
☒	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 5 recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
☒	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
☒	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
☐	Contracts with customers establish DOC ownership rights over data including PII/BII.
☐	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
☐	Other (specify):

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

PII within the system is secured using appropriate management, operational, and technical safeguards in accordance with NIST requirements. Such management controls include a review process to ensure that management controls are in place and documented in the System Security Privacy Plan (SSPP). The SSPP specifically addresses the management, operational, and technical controls that are in place and planned during the operation of the system. Operational safeguards include restricting access to PII/BII data to a small subset of users. All access has role-based restrictions and individuals with access privileges have undergone vetting and suitability screening. Data is maintained in areas accessible only to authorized personnel. The system maintains an audit trail and the appropriate personnel is alerted when there is suspicious activity. In addition:

- Data is encrypted in transit through HTTPS.
- Data transfer is secured through Transport Layer Security (TLS) 1.2
- Linux servers within PSS-SS are regularly updated with the latest security patches by the Linux System Support Groups.

PSS-SS utilizes Enterprise Directory Services (EDS) which is an industry standards-based authentication, authorization, and accounting directory data source for user credentials based

on Active Directory and, increasingly, Oracle Unified Directory, which provides authorized USPTO personnel access to their workstation, email, Internet, network servers, Virtual Private Network (VPN), and AISs throughout the USPTO. EDS has increased application and system security, while reducing administrative, implementation, and maintenance costs of AISs. EDS facilitates the centralized management of personnel, customer, and partner information, which ensures information consistency and provides a capability for RBAC.

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.)*

General Records Schedules (GRS) | National Archives

☒	There is an approved record control schedule. Provide the name of the record control schedule: N1-241-10-01:2 Patent Case Files, Granted N1-241-10-01:5.1 Patent Cooperation Treaty (PCT) Applications and Miscellaneous Records N1-241-10-1:10.1 Patent Classification Files
☐	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: PSS-SS contains PII/BII data identified in 2.1 that combined can identify a person.
☒	Quantity of PII	Provide explanation: The quantity of PII/BII identified in 2.l in PSS-SS applications determined categorization at a moderate impact level.
☒	Data Field Sensitivity	Provide explanation: PSS-SS contains PII/BII data identified in 2.1 that combined can identify a person.
☒	Context of Use	Provide explanation: PSS-SS is made up of applications that allow patent examiners and applicants to effectively search the USPTO patent data repositories. (Including bulk/services exchanges)

☒	Obligation to Protect Confidentiality	Provide explanation: USPTO Privacy Policy requires the PII information collected within the system to be protected accordance to NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information. In accordance with the Privacy Act of 1974, PII must be protected.
☒	Access to and Location of PII	Provide explanation: The information captured, stored, and transmitted by PSS-SS applications 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