Version Number: 01-2020

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

Privacy Impact Assessment
for the
Patent Search System – Primary Search and Retrieval (PSS-PS) 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 02/17/2021

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO Patent Search System – Primary Search & Retrieval (PSS-PS)

Unique Project Identifier: PTOP-008-00

Introduction: System Description

Provide a description of the system that addresses the following elements:
Patent Search System-Primary Search and Retrieval (PSS-PS), is a Major system, which supports the Patent Cost Center. It is considered a mission critical "system." It consist of Search and Retrieval automation tools that provide 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.

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

PSS-PS is a major application.

(b) System location

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-PS interconnects with the following systems:
Enterprise Windows Services (EWS): The EWS is an infrastructure information system, and provides a hosting platform for major applications that support various USPTO missions.

Enterprise UNIX Service (EUS): The EUS System consists of assorted UNIX operating system variants (OS), each of which is 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, and provides an aggregate of subsystems that facilitates the communications, secure access, protective services, and network infrastructure support for all United States Patent and Trademark Office (USPTO) IT applications.

Patent Capture and Application Processing System – Initial Processing (PCSPS-IP): The PCAPS-IP is an Application information system, and 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 the patent applications. PCAPS-IP is comprised of multiple Automated Information Systems (components) that perform specific functions, including submissions, categorization, metadata capture, and patent examiner assignment of patent applications.

Patent Capture and Application Processing System – Examination Support (PCAPS-ES): The PCAPS-ES is an information system composed of 20 Components: Electronic Business Center Imaging System, Electronic Desktop Application Navigator, File Inspection Utility, Image File Wrapper, Office Action Correspondence System, Patent Resource Management System, PAIR User Resource Manager, Patent Application Location Monitoring – Examination and Post-Examination, Patent Application Location Monitoring-Services Gateway, Patent Application Location Monitoring – File Ordering System, Patent Application Location Monitoring- Infrastructure, Patent Application Information Retrieval-Private, Patent Enterprise Access Integration Public Patent Application Information Retrieval-Public, Trilateral Document Access, Patent File Wrapper, Quality Review System, Supplemental Complex Repository for Examiners, Technology Assessment and Forecast, Patents Telework Enterprise System, & Integrated Quality System.

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

Service Oriented Infrastructure (SOI): The SOI provides a feature-rich and stable platform upon which USPTO applications can be deployed.

Enterprise Software System (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): 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, & Situational Awareness and Incident Response.

Database Services (DBS): The DBS is an infrastructure information system, and provides a Database Infrastructure to support mission of USPTO database needs.

Trilateral Network (TRINET): TRINET is an Infrastructure information system, and provides secure network connectivity for electronic exchange and dissemination of sensitive patent data between authenticated endpoints at the Trilateral Offices and TRINET members. The Trilateral

Offices consist of the United States Patent and Trademark Office (USPTO), the European Patent Office (EPO), and the Japanese Patent Office (JPO). The TRINET members consist of the World Intellectual Property Office (WIPO), the Canadian Intellectual Property Office (CIPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO) and the Intellectual Property Office of Australia (IPAU).

Patent End to End (PE2E): Patents End-to-End (PE2E) is a Master system portfolio consisting of next generation Patents Automated Information Systems (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 will be a single web-based examination tool providing users with a unified and robust set of tools. PE2E will overhaul the current patents examination baseline through the development of a new system that replaces the existing tools used in the examination process.

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

PSS-PS supports legal determinations of prior art for patent applications, including text and image searches of repositories of US application and grant publications, Foreign application and grant publications, various concordances, and non-patent literature. It represents the databases that contain the images and text data for US Patent Grants, Published applications, and unpublished applications. This area includes the examiner interfaces that provide the search capability through East and West.

The PSS-PS master system has multiple AIS's with search and retrieval automation tools that supports the USPTO Patent examiners legal determination of prior art of patent applications.

The AIS's are:
Application Image Retrieval System (AIRS): The purpose of AIRS is to provide patent application images and metadata to the following subsystems: Examiners Automated Search Tool (EAST), Hypertext Transfer Protocol Print Service (HPS), Order entry Management System (OEMS) and the Web Examiner's Search Tool (WEST).

Application Images on the Web (AIW): AIW is an internet application that runs outside the USPTO firewall and provides an access point for public users to retrieve domestic patent

application images. The purpose of AIW is to provide images and metadata to the Application Full-Text (AppFT) subsystem.

The Patent Image Retrieval System (PIRS): The purpose of PIRS is to provide Patent images and metadata to the following subsystems: EAST, HPS, OEMS, and WEST.

Patent Images on the Web (PIW): PIW is an internet application that runs outside the USPTO firewall and provides an access point for public users to retrieve domestic Patent images. The purpose of PIW is to provide images and metadata to the Patents Full-Text (PatFT) subsystem.

Web-based Examiner's Search Tool (WEST): WEST is a Web browser-based client interface, which utilizes HTTP as a front end to the Bibliographic Retrieval System (BRS) database system. It operates over the USPTO Transmission Control Protocol/Internet Protocol (TCP/IP) Intranet (PTONet). This intranet tool also supports text search capabilities and retrieval functions of abstracts, images, and full-text patent documents from other domestic, international, and commercial databases.

PubWEST: PubWEST is the publicly-accessible version of WEST. PubWEST, similarly to WEST, provides search access to most USPTO patent text searchable databases.

Enterprise Text Search 1(ETS1): The ETS1 system is a continuation of the BRS Middle-tier Phase 1 and BRS Middle-tier Phase 2 systems. ETS1 is a multi-tiered application that improves the scalability and the performance of the BRS search system while using fewer system resources.

Examiners Automated Search Tool (EAST): A single user interface that can be used to search for prior art of any type, this application integrates with other activities performed by patent examiners to reduce the time required to examine applications. EAST provides full text and abstract text data search and retrieval of domestic and international, commercial and government databases using the BRS search engine.

Public Examiners Automated Search Tool (PubEAST): This application is the publicly-available version of EAST. It provides search request capability for most USPTO patent text searchable databases to public users. It has full text search capabilities from the following databases: USPAT, USOCR, EPO, and JPO text/image databases.

Patent Linguistic Utility Search (PLUS): PLUS uses the BRS query by example technology to compare keywords in a patent application to keywords in published patent applications and granted patents. Search results include matching patent and/or patent application numbers, and

classification and sub-classification for patents matched, along with relevance ranking for the match.

European Patent Office Query System (EPOQUE): EPOQUE connects to the Trilateral Secure Virtual Private Network (TSVPN), part of the USPTO Trilateral Network (TriNet), to access and allow queries from US Patent Examiners and other users to the European Patent Office (EPO) at The Hague, Netherlands.

HTTP Print Service (HPS): HPS allows USPTO internal users and users in the public search rooms to print patent/publication application images to designated Windows-based group printers.

Applications Full-Text (AppFT): A standalone internet application that runs outside of the USPTO firewall and provides general public access to Pre-Grant, published patent applications. It connects to the PGPub/CSS application and AIW for images.

Patent Full Text on the Web (PATFT): A stand-alone internet application, which allows the general public to search and retrieve granted US patents. It runs outside the USPTO firewall with a copy of the USPTO BRS database that is provided to USPTO examiners.

Classification Data System (CDS): CDS is a collection of applications and processes which support the capture and maintenance of patent and PGPub classification data of US documents as well as the maintenance of the USPC. CDS also supports the maintenance of the US-to-IPC Concordance and Limited Family data and is the data source of several classification publications.

Computer Search Systems (CSS): CSS is a set of databases, conversion and load software, data administration tools, and procedures to maintain and keep available a number of internal, external, government, and commercial databases for text search and retrieval via other USPTO applications.

Electronic Patent Reference (EPR): This is a single-user, client application that is downloaded on-demand from a Patent Application Information Retrieval (PAIR) server and installed on public personal computers. It provides patent references from PIW and AIW to applicants via a Private PAIR system.

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

Information in the system is retrieved through internet access and a registered account.

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

Information is transmitted to and from PSS-PS via the internet and internal USPTO network.

(g) Any information sharing conducted by the system

The PSS-PS does not conduct any information sharing.

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

- 35 U.S.C. 115
- 35 U.S.C.2
- 5 U.S.C. 301

(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 (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*	☐	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. Physical Characteristics	☐
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 EMSO provide additional automated transmission and monitoring mechanisms to ensure that PII/BII information is protected and not breached by external entities.

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
☐	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):			

☒	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): 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).

The data collected facilitates access for public users to search the USPTO Patent data repositories, which allows
- The general public to search and retrieve domestic application images
- Patent examiners and applicants to identify individuals and organizations with Intellectual property, pre-grant, and published applications.

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.)

Inadvertent PII/BII exposure and the 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.

USPTO requires annual security role-based training and annual mandatory security awareness procedure training for all employees. The following are USPTO's current policies: Information Security Foreign Travel Policy (OCIO-POL-6), IT Privacy Policy (OCIO-POL-18), IT Security Education Awareness Training Policy (OCIO-POL-19), Personally Identifiable Data Removal Policy (OCIO-POL-23), and USPTO Rules of the Road (OCIO-POL36). All offices of USPTO adhere to 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: System Name / Organization PCAPS-ES / USPTO PCAPS-IP / USPTO PE2E / USPTO By restricting access to the system via Activity Directory, PSS-PS, PCAPS-ES, PCAPS-IP, and PE2E's protection of PII data is performed by the implemented AD automated system. Automatic quality control

	for data checks exists. VPN is used for developer access. There is a network connection to the internet via the Network Perimeter for PSS-PS and PSS-SS users. PSS-PS, PSS-SS, PCAPS-ES, PCAPS-IP 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-PS, PSS-SS, PCSPS-ES, PCAPS-IP. This connection is protected and controlled by the USPTO infrastructure.
☐	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: http://www.uspto.gov/privacy-policy	
☐	Yes, notice is provided by other means.	Specify how:
☒	No, notice is not provided.	Specify why not: PSS-PS 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 and patent owner(s) consent were previously obtained during initial patent filing.

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-PS 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 and patent

		owner(s) consent were previously obtained during initial patent filing.

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-PS 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 and patent owner(s) consent were previously obtained during initial patent filing.

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-PS 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.)*

☐	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: In addition to security and management controls to prevent the inappropriate disclosure of sensitive information. USPTO implements the Perimeter Network (NSI) and EMSO to provide automated transmission and monitoring mechanisms to ensure that PII/BII information is protected and

	not breached by external entities.
☒	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): _____9/16/2020____ ☐ 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 is protected with operational and technical controls that are documented in the PSS-PS System Security Plan. A Security Categorization compliant with the FIPS 199 and NIST SP 800-60 requirements was conducted for PSS-PS. The overall FIPS 199 security impact level for PSS-PS was determined to be Moderate. This categorization influences the level of effort needed to protect the information managed and transmitted by the system.

A. Operational controls include securing all hardware associated with the PSS-PS 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.
B. Backups are managed by the Enterprise Tape Backup System (ETBS) and are secured off-site by First Federal.
C. Windows and Linux servers within PSS-PS 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
☐	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 FY2018
☐	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, home address, work address, work email, work phone number and user id are the non-sensitive PII that could be used to identify an individual.
☐	Quantity of PII	Provide explanation:
☒	Data Field Sensitivity	Provide explanation: Non-sensitive PII.
☒	Context of Use	Provide explanation: The data is for official correspondences between the applicant and USPTO. Once a patent is granted the patent owner and patent examiner correspondence information is included as a matter for public record purposes. This public information will return whenever a public users use PSS-PS online public search tools (i.e., PatFT, AppFT, AIW, PIW).
☐	Obligation to Protect Confidentiality	Provide explanation:
☐	Access to and Location of PII	Provide explanation:
☐	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.)

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.