Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
Patent Examination Data Search (PEDS)

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

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

Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry
Date: 2023.09.06 13:10:53 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO Patent Examination Data Search (PEDS)

Unique Project Identifier: PTOP-012-00

Introduction: System Description

Provide a brief description of the information system.

The Patent Examination Data system (PEDS) is a platform in Amazon Web Services US (AWS) East/West to provide bulk download of patent bibliographic data in a secure manner without impacting USPTO internal users.

The demand for bulk patent examination data continues to be one of the top public service requests. Bulk patent application data is of high value to law firms, technology companies, researchers and data resellers. Provision of bulk patent examination data continues to be a key component of the USPTO's compliance with the President's Open Government Initiative.

As a result, PEDS was released permitting public users to search and download bibliographic application data, published documents, Patent Term Extension data, images and transaction history provided in bulk.

Address the following elements:

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

(b) System location
PEDS is hosted on AWS East/West USPTO Virtual Private Cloud (VPC).

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
PEDS interconnects with Patent Capture and Application Processing System – Examination Support (PCAPS-ES) and ingests non-sensitive patent application and bibliographic data from PCAPS-ES.
PCAPS-ES: The purpose of this system is to process, transmit and store data and images to support the data-capture and conversion requirements of the USPTO to support the USPTO patent application process.

NSI (Network and Security Infrastructure System): 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.

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

USPTO AWS Cloud Services (UACS) EIPL-IHSC: The UACS General Support System (GSS) is a standard infrastructure platform used to support PTO Application Information Systems (AIS) hosted in the AWS East/West environment.

Database Services (DBS ORACLE): provides a Database infrastructure to support the mission of USPTO Database needs. The DBS System is composed of a collection of various versions of Database systems. The subsystems within the DBS System includes: SQL Database Servers (MSSQL); Oracle (Oracle); and MySQL (MySQL). No PII.

(d) The way the system operates to achieve the purpose(s) identified in Section 4
Customers download datasets using a web interface or Application Programming Interface (API) calls in XML (extensible markup language) or JSON (JavaScript Object Notation) formats. PEDS is updated daily.

(e) How information in the system is retrieved by the user
Customers download datasets using a web interface or Application Program interface (API) calls in XML (extensible markup language) or JSON (JavaScript Object Notation) formats.

(f) How information is transmitted to and from the system
Customers download datasets using a web interface or API calls in XML or JSON formats. A one-way connection is made from the source database to the application database for data ingestion and updates.

(g) Any information sharing
PEDS ingests non-sensitive PII data from PCAPS-ES and disseminates the data directly to the public web interface or API.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information
35 USC 122(b); 35 U.S.C. 151; 37 CFR 1.14

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

The FIPS 199 security impact category for this system is low.

Section 1: Status of the Information System

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

☐ This is a new information system.

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

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions	☐	d. Significant Merging	☐	g. New Interagency Uses	☐
b. Anonymous to Non-Anonymous	☐	e. New Public Access	☐	h. Internal Flow or Collection	☐
c. Significant System Management Changes	☐	f. Commercial Sources	☐	i. Alteration in Character of Data	☐
j. Other changes that create new privacy risks (specify):					

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

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

Section 2: Information in the System

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

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

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

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

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

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

Other Information (specify)

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

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

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 Security and Compliance Services (SCS) provide additional automated transmission and monitoring mechanisms to ensure that PII/BII information is protected and not breached by external entities. PII pertaining to individuals can be reviewed within PEDS. PII cannot be updated in PEDS. The individual will have to contact PTO helpdesk to update their information. Once the PII has been updated in the front-end system, PEDS information will be updated during the next data sync.

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): None Apply.			

☒	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings	☐	Building entry readers	☐
Video surveillance	☐	Electronic purchase transactions	☐
Other (specify): Click or tap here to enter text.			

☒	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program	☐	For administering human resources programs	☐
For administrative matters	☒	To promote information sharing initiatives	☒
For litigation	☐	For criminal law enforcement activities	☐
For civil enforcement activities	☐	For intelligence activities	☐
To improve Federal services online	☒	For employee or customer satisfaction	☒
For web measurement and customization technologies (single-session)	☐	For web measurement and customization technologies (multi-session)	☐
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

Bulk patent application data is of high value to law firms, technology companies, researchers and data resellers for searching and downloading bibliographic application data, published documents, Patent Term Extension data, images and transaction history. PEDS enables public users to bulk download bibliographic data from issued patents and public patent applications. The PII/BII identified in Section 2.1 is in reference to any patent applicant and/or patent owner or patent practitioner and can be categorized as one or combination of the following: (i) federal employee, (ii) contractors (during the development phase alone), (iii) members of the public, or (iv) foreign national who will have access since PEDS is open to the public.

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.)

USPTO has identified and evaluated potential threats to privacy and determined they are insider threats and foreign entities. There is a need to protect the confidentiality and integrity of the PII that is collected since it could be requested during a criminal investigation. PEDS data is protected through the use of access control permissions and next generation firewall, anti-virus, and host intrusion detection systems. USPTO has implemented NIST security controls (encryption, access control, auditing) and mandates IT Awareness and role-based training for staff who have access to the system and address how to handle, retain, and dispose of data adequately.

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

Comprehensive Records Schedule or the General Records Schedule and the corresponding disposition authorities or citations.

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: PCAPS-ES: By restricting access to the system via Activity Directory (AD), PCAPS-ES 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. PCAPS-ES 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 PCAPS-ES. This connection is protected and controlled by the USPTO infrastructure. NSI (Network and Security Infrastructure System): 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. Security and Compliance Services (SCS): SCS provides Security Incident and Event Management, Enterprise Forensic, Enterprise Management System, Security and Defense, Enterprise Scanner, Enterprise Cybersecurity Monitoring Operations, Performance Monitoring Tools, Dynamic Operational Support Plan, & Situational Awareness and Incident Response. USPTO AWS Cloud Services (UACS) EIPL-IHSC: The UACS General Support System (GSS) is a standard infrastructure platform used to support PTO Application Information Systems (AIS) hosted in the AWS East/West environment. Database Services (DBS ORACLE): provides a Database infrastructure to support the mission of USPTO Database needs. The DBS System is composed of a collection of various versions of Database systems. The subsystems within the DBS System includes: SQL Database Servers (MSSQL); Oracle (Oracle); and MySQL (MySQL). No PII. NIST security controls are in place to ensure that information is handled, retained, and disposed of appropriately. For example, advanced encryption is used to secure the data both during transmission and while stored at rest. Access to individual's PII is controlled through the application and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. USPTO requires annual security role based training and annual mandatory security awareness procedure training for all employees. All offices adhere to the USPTO Records Management Office's Comprehensive Records Schedule or the General Records Schedule and the corresponding disposition authorities or citations.
☐	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

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

Class of Users			
General Public	☒	Government Employees	☒
Contractors	☐		
Other (specify):			

Section 7: Notice and Consent

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

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

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

☐	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
☒	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: Individuals do not have an opportunity to decline to provide PII because PEDS does not require users to provide any PII/BII directly, PEDS only disseminates the data collected from other systems. Patent owner name, correspondence address, etc. that returns during searches are available for public record and patent applicant/owner consent was previously obtained during initial patent filing through the front end systems.

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: Individuals do not have an opportunity to consent to particular uses of their PII because PEDS does not require users to provide any PII/BII directly, PEDS only disseminates the data collected from other systems. Patent owner name, correspondence address, etc. that returns during searches are available for public record and patent applicant/owner consent was previously obtained during initial patent filing through the front end systems.

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

☒	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: PII pertaining to individuals can be reviewed within PEDS. PII cannot be updated in PEDS. The individual will have to contact PTO helpdesk to update their information. Once the PII has been updated in the front end system, PEDS information will be updated during the next data sync.
☐	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

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

☐	All users signed a confidentiality agreement or non-disclosure agreement.
☐	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
☒	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
☐	Access to the PII/BII is restricted to authorized personnel only.
☒	Access to the PII/BII is being monitored, tracked, or recorded. Explanation:
☒	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 7/1/2022 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
☐	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
☒	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
☒	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
☒	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
☐	Contracts with customers establish DOC ownership rights over data including PII/BII.
☐	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
☒	Other (specify):

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

The PCAPS-ES that PEDS ingests data from collects voluntary applicant correspondence information to facilitate direct communications between the applicants and the Office. PCAPS-ES applications are managed and secured by the USPTO's Active Directory (AD) and Unix Enterprise infrastructure and other OCIO established technical controls that include password authentication at the server and database levels. HTTPS is used for all data transmissions to and from the Internet, USPTO DMZ, and PTONet . A dedicated socket is used to perform encryption and decryption.

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)*: • COMMERCE/PAT-TM-7, Patent Application Files • COMMERCE/PAT-TM-9, Patent Assignment Records • COMMERCE/PAT-TM-23, User Access for Web Portals and Information Requests
☐	Yes, a SORN has been submitted to the Department for approval on (date).
☐	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

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

☒	There is an approved record control schedule. Provide the name of the record control schedule: Evidentiary Patent Applications N1-241-10-1:4.1 Patent Examination Working Files N1-241-10-1:4.2

	Patent Examination Feeder Records N1-241-10-1:4.4 Patent Post-Examination Feeder Records N1-241-10-1:4.5 Patent Case Files, Granted N1-241-10-1:2 Abandoned Patent Applications, Not Referenced in Granted Case File N1-241-10-1:3
☐	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
☒	Yes, retention is monitored for compliance to the schedule PCAPS-ES.
☐	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, telephone, email address are all personal identifiers and can identify a particular individual.
☒	Quantity of PII	Provide explanation: Millions of patent application data can be found within PEDS.
☒	Data Field Sensitivity	Provide explanation: The combination of the data fields do not make the data more sensitive.
☒	Context of Use	Provide explanation:

		The demand for bulk patent examination data continues to be one of the top public service requests. Bulk patent application data is of high value to law firms, technology companies, researchers and data resellers. Provision of bulk patent examination data continues to be a key component of the USPTO's compliance with the President's Open Government Initiative. As a result, PEDS was released permitting public users to search and download bibliographic application data, published documents, Patent Term Extension data, images and transaction history provided in bulk.
☒	Obligation to Protect Confidentiality	Provide explanation: There is no obligation to protect confidentiality of the PII, the PII processed by PEDS is public record information.
☒	Access to and Location of PII	Provide explanation: The information within PEDS is publicly available through the worldwide web via ped.uspto.gov
☐	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

The potential threats to privacy are foreign entities and insider threats. The information in PEDS is for public consumption and a Privacy Act Statement attached to all patent applications indicates the voluntary nature of PII data submission and the authorities authorizing public use of the PII including those listed in appendix A below.

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

A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.