

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



**Privacy Impact Assessment
for the
Global Patent Solutions (GPS) System**

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

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

Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry
Date: 2021.08.13 13:34:11 -04'00'

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

Date

U.S. Department of Commerce Privacy Impact Assessment USPTO Global Patent Solutions (GPS) System

Unique Project Identifier: PTOC-024-00

Introduction: System Description

The GPS is an information system that provides support to the USPTO patent review process. The GPS system is designed to support the USPTO international application or Patent Cooperation Treaty (PCT) application process. The PCT provides a unified procedure for filing patent applications to protect inventions in each of its Contracting States. The GPS system facilitates PCT searches and enables GPS employees to submit an accompanying written opinion regarding the patentability of the invention in question.

GPS is under contract with the USPTO to perform work that is related to PCT applications. GPS receives PCT application data from the USPTO via secure file transfer protocol (FTP) using the Tumbleweed File Transfer Application. Using this data, GPS conducts searches and develops opinion papers in support of the USPTO contract.

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

GPS Automated Information System (GPS system) is a major application.

(b) System location

GPS is located in Scottsdale, Arizona and the AWS FedRAMP-approved cloud.

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

GPS interconnects with the USPTO File Transfer System. PCT applications and PCT opinions are shared only between the GPS system and the USPTO through the secure connection managed by the USPTO. PCT data is exported from USPTO PCT Operations (PCT OPS) application information system (AIS). The GPS system receives the PCT application data from the USPTO via secure file transfer protocol, with an encrypted SSL connection. This secure connection is managed by the USPTO.

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

The GPS is an information system that provides support to the USPTO patent review process. The GPS system is designed to support the USPTO international application or Patent

Cooperation Treaty (PCT) application process. The PCT provides a unified procedure for filing patent applications to protect inventions in each of its Contracting States. The GPS system facilitates PCT searches and enables GPS employees to submit an accompanying written opinion regarding the patentability of the invention in question. GPS operates by receiving PCT applications from USPTO, storing the data, and distributing it to GPS staff to conduct searches and examination. Completed deliverables are returned from GPS to USPTO.

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

GPS receives the information from USPTO via secure file transfer. Assigned applications are accessed by analysts who connect to GPS hosted on AWS via Virtual Private Network (VPN) and Remote Desktop Protocol (RDP). Completed applications are returned to USPTO.

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

Patent data is imported/exported from/to the GPS GSS via Secure Shell (SSH) File Transfer Protocol (SFTP) provided by USPTO.

(g) Any information sharing conducted by the system

GPS shares information with USPTO only.

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

35 U.S.C. 1, 2, 6, 41, 115, and 261; E.O. 9424; 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	<input type="checkbox"/>	d. Significant Merging	<input type="checkbox"/>
		e. New Interagency Uses	<input type="checkbox"/>

b. Anonymous to Non-Anonymous	<input type="checkbox"/>	e. New Public Access	<input type="checkbox"/>	h. Internal Flow or Collection	<input type="checkbox"/>
c. Significant System Management Changes	<input type="checkbox"/>	f. Commercial Sources	<input type="checkbox"/>	i. Alteration in Character of Data	<input type="checkbox"/>
j. Other changes that create new privacy risks (specify):					

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

Section 2: Information in the System

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

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

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

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

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

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

Other Information (specify)					

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

Directly from Individual about Whom the Information Pertains					
In Person	<input type="checkbox"/>	Hard Copy: Mail/Fax	<input type="checkbox"/>	Online	<input type="checkbox"/>
Telephone	<input type="checkbox"/>	Email	<input type="checkbox"/>		
Other (specify):					

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

Non-government Sources					
Public Organizations	<input type="checkbox"/>	Private Sector	<input type="checkbox"/>	Commercial Data Brokers	<input type="checkbox"/>
Third Party Website or Application			<input type="checkbox"/>		
Other (specify): Members of the public					

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

<p>GPS connects to the USPTO File Transfer system, which is a part of the Network and Security Infrastructure (NSI) Master System.</p> <p>USPTO data is received by way of a secured file transfer using Tumbleweed. When USPTO data is transferred to GPS through this connection, GPS-authorized staff members will validate the data received and save it to the appropriate virtual storage device. Access to the virtual storage device where USPTO data is stored is strictly controlled using Active Directory groups. The Research Analysts will access the data from the virtual storage device via RDS. When the work deliverables are approved by a Search Approval Official, the Docket Manager transmits the work deliverables via the same secured file transfer back to the USPTO.</p> <p>In accordance with the USPTO Privacy Policy guidelines, the GPS system is designed and administered to ensure the integrity of PII provided to GPS by USPTO. Bibliographic data (Inventor name, Inventor address, Citizenship, Correspondence address, Employer name and address, Telephone number[s], and Email address) are collected from the applicant or applicant’s legal representative and attached to the electronic patent application files sent to GPS.</p> <p>Specific safeguards that are employed by GPS to protect the patent applications include:</p> <ul style="list-style-type: none"> • The GPS system and its facility are physically secured and closely monitored. Only individuals authorized by GPS to access USPTO data are granted logical access to the system. • All patent information is encrypted when transferred between GPS and USPTO using secure electronic methods. • All patent information is encrypted at rest. • Technical, operational, and management security controls are in place at GPS and are verified regularly. • Periodic security testing is conducted on the GPS system to help ensure that any new security vulnerabilities are discovered and fixed. • All GPS personnel are required to take security training.

2.4 Is the information covered by the Paperwork Reduction Act?

<input checked="" type="checkbox"/>	<p>Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.</p> <p>0651-0031 Patent Processing 0651-0032 Initial Patent Application</p>
<input type="checkbox"/>	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. (Check all that apply.)

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards	<input type="checkbox"/>	Biometrics	<input type="checkbox"/>
Caller-ID	<input type="checkbox"/>	Personal Identity Verification (PIV) Cards	<input type="checkbox"/>
Other (specify):			

<input checked="" type="checkbox"/>	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.
-------------------------------------	--

Section 3: System Supported Activities

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

Activities			
Audio recordings	<input type="checkbox"/>	Building entry readers	<input type="checkbox"/>
Video surveillance	<input type="checkbox"/>	Electronic purchase transactions	<input type="checkbox"/>
Other (specify):			

<input checked="" type="checkbox"/>	There are not any IT systems supported activities which raise privacy risks/concerns.
-------------------------------------	---

Section 4: Purpose of the System

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

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

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 PII/BII that is collected is used to identify PCT patent applicants. The information is collected and disseminated by the Patent ingress systems owned and operated by USPTO. The GPS system does not disseminate this information outside of the organization. The PII/BII may come from persons applying for and reviewing patents through the USPTO who are considered members of 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.)

The potential threats to the system are insider threats, adversarial entities and foreign governments. To mitigate threats GPS has implemented the following:

- The GPS system and its facility are physically secured and closely monitored. Only individuals authorized by GPS to access USPTO data are granted logical access to the system.
- All patent information is encrypted when transferred between GPS and USPTO using secure electronic methods.
- All patent information is encrypted at rest.
- Technical, operational, and management security controls are in place at GPS and are verified regularly.
- Data Loss Prevention (DLP) technology is used to prevent dissemination of data.
- Periodic security testing is conducted on the GPS system to help ensure that any new security vulnerabilities are discovered and corrected/mitigated.
- All GPS personnel are required to take security training.

Section 6: Information Sharing and Access

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

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
DOC bureaus	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Federal agencies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

<input type="checkbox"/>	The PII/BII in the system will not be shared.
--------------------------	---

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

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

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

<input checked="" type="checkbox"/>	<p>Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII.</p> <p>Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:</p> <p>GPS connects to the USPTO File Transfer system, which is a part of the NSI Master System. In accordance with the USPTO Privacy Policy guidelines, the GPS system is designed and administered to ensure the confidentiality of PII provided to GPS by USPTO. Bibliographic data (Inventor name, Inventor address, Citizenship, Correspondence address, Employer name and address, Telephone number[s], and email address) are collected from the applicant or applicant's legal representative and attached to the electronic patent application files sent to GPS. During processing, the information is passed to various stages of the GPS workflow. The information is not shared with any entity outside of GPS operational facility.</p> <p>Specific safeguards that are employed by GPS to protect the patent applications include:</p> <ul style="list-style-type: none"> • The GPS system and its facility are physically secured and closely monitored. Only individuals authorized by GPS to access USPTO data are granted logical access to the system. • All patent information is encrypted using secure electronic methods when transferred between GPS and USPTO. • Technical, operational, and management security controls are in place at GPS and are verified regularly. • Periodic security testing is conducted on the GPS system to help ensure that any new security vulnerabilities are discovered and fixed. • All GPS personnel are required to take security training.
-------------------------------------	---

<input type="checkbox"/>	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.
--------------------------	---

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

Class of Users			
General Public	<input type="checkbox"/>	Government Employees	<input checked="" type="checkbox"/>
Contractors	<input checked="" type="checkbox"/>		
Other(specify):			

Section 7: Notice and Consent

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

<input checked="" type="checkbox"/>	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
<input checked="" type="checkbox"/>	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://www.uspto.gov/privacy-policy .	
<input type="checkbox"/>	Yes, notice is provided by other means.	Specify how:
<input type="checkbox"/>	No, notice is not provided.	Specify why not:

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

<input type="checkbox"/>	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: The option for individuals to review or update PII/BII pertaining to them can only be offered by the primary patent application ingress system. That information is volunteered by individuals as a part of the patent application process.

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

<input type="checkbox"/>	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: That option would be offered by the primary patent application ingress system.

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

<input type="checkbox"/>	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how:
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: The option for individuals to review or update PII/BII pertaining to them can only be offered by the primary patent application ingress system. Individuals have an opportunity to review/update PII/BII pertaining to them up to and before the patent application is published and finalized.

Section 8: Administrative and Technological Controls

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

<input checked="" type="checkbox"/>	All users signed a confidentiality agreement or non-disclosure agreement.
<input checked="" type="checkbox"/>	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
<input checked="" type="checkbox"/>	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
<input checked="" type="checkbox"/>	Access to the PII/BII is restricted to authorized personnel only.
<input checked="" type="checkbox"/>	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: The 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.
<input checked="" type="checkbox"/>	The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): <u>10/22/2020</u> <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
<input checked="" type="checkbox"/>	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
<input checked="" type="checkbox"/>	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
<input checked="" type="checkbox"/>	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
<input checked="" type="checkbox"/>	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
<input checked="" type="checkbox"/>	Contracts with customers establish DOC ownership rights over data including PII/BII.
<input checked="" type="checkbox"/>	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
<input type="checkbox"/>	Other (specify):

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

Access to the system and data are limited to examiners, management, and system administrators. Data is received, processed through the GPS workflow, used to aid PCT searches and written opinions, and returned to USPTO. All transfers of data between GPS and USPTO occur over a FIPS 140-2-certified secure file transport system. The GPS data transfer system uses strong encryption to ensure secure transmission of sensitive data between USPTO and the GPS information system. All PII/BII stored within the system is encrypted at rest by the file server.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

- Yes, the PII/BII is searchable by a personal identifier.
- No, the PII/BII is not searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, “the term ‘system of records’ means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.”

<input checked="" type="checkbox"/>	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. <i>(list all that apply):</i> PAT/TM—1 Attorneys and Agents Registered or Recognized to Practice Before the Office PAT/TM—7 Patent Application Files PAT/TM—9 Patent Assignment Records PAT/TM—10 Deposit Accounts and Electronic Funds Transfer Profiles
<input type="checkbox"/>	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
<input type="checkbox"/>	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

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

<input checked="" type="checkbox"/>	There is an approved record control schedule. Provide the name of the record control schedule: Patent Cooperation Treaty (PCT) Applications and Miscellaneous Records (N1-241-10-1:5.1) Patent Examination Working Files (N1-241-10-1:4.2)
<input type="checkbox"/>	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:
<input checked="" type="checkbox"/>	Yes, retention is monitored for compliance to the schedule.
<input type="checkbox"/>	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	<input type="checkbox"/>	Overwriting	<input checked="" type="checkbox"/>
Degaussing	<input type="checkbox"/>	Deleting	<input checked="" type="checkbox"/>
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

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

11.2 Indicate which factors were used to determine the above PII confidentiality impact level. *(Check all that apply.)*

<input checked="" type="checkbox"/>	Identifiability	Provide explanation: The combination of occupation, name, title, address, phone number, citizenship status & email address can easily identify a
-------------------------------------	-----------------	---

		particular individual.
<input checked="" type="checkbox"/>	Quantity of PII	Provide explanation: The number of data items collected is large enough to warrant concern.
<input checked="" type="checkbox"/>	Data Field Sensitivity	Provide explanation: The data includes limited personal and work-related elements but could make the information more sensitive when combined.
<input checked="" type="checkbox"/>	Context of Use	Provide explanation: Information is used to facilitate PCT searches by contractors working outside of the USPTO environment.
<input checked="" type="checkbox"/>	Obligation to Protect Confidentiality	Provide explanation: USPTO employees (including contractors) undergo annual cyber security awareness training related to the proper handling of PII/BII within the USPTO and are obligated by the organizational rules related to handling PII/BII.
<input checked="" type="checkbox"/>	Access to and Location of PII	Provide explanation: Because the information containing PII must be transmitted outside of the USPTO environment, there is an added need to ensure the confidentiality of information during transmission.
<input type="checkbox"/>	Other:	Provide explanation:

Section 12: Analysis

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

Potential threats to the information system are insider threats, foreign governments and adversarial entities. GPS connects to the USPTO File Transfer system, which is a part of the NSI Master System. In accordance with USPTO Privacy Policy guidelines, the GPS system is designed and administered to ensure the confidentiality and integrity of PII provided to GPS by USPTO. The GPS system and its facility are physically secured and closely monitored. Only individuals authorized by GPS to access USPTO data are granted access to the system. All PCT information is encrypted when transferred between GPS and USPTO using secure electronic methods. Technical, operational, and management security controls are in place at GPS and are verified regularly. Periodic security testing is conducted on the GPS system to help assure that any new security vulnerabilities are discovered and fixed. All GPS personnel are trained to securely handle patent information and to understand their responsibilities for protecting patents. The type or quantity of information collected and the sources providing the information is done prior to GPS involvement. GPS converts the information given to them by USPTO and is not privy to the decision making process within USPTO regarding information collected.

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

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

<input checked="" type="checkbox"/>	No, the conduct of this PIA does not result in any required business process changes.
-------------------------------------	---

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

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

USPTO Points of Contact and Signatures

<p>System Owner Name: Harry Kim Office: International Patent Legal Administration (IPLA) Phone: (571) 272-3285 Email: Harry.Kim@uspto.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: <u>Users, Kim, Harry</u> <small>Digitally signed by Users, Kim, Harry Date: 2021.07.28 11:07:43 -04'00'</small></p> <p>Date signed: _____</p>	<p>Chief Information Security Officer Name: Don Watson Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-8130 Email: Don.Watson@uspto.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: <u>DON R Watson</u> <small>Digitally signed by DON R Watson Date: 2021.07.29 09:37:16 -04'00'</small></p> <p>Date signed: _____</p>
<p>Privacy Act Officer Name: John Heaton Office: Office of General Law (O/GL) Phone: (571) 270-7420 Email: Ricou.Heaton@uspto.gov</p> <p>I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA.</p> <p>Signature: <u>Users, Heaton, John (Ricou)</u> <small>Digitally signed by Users, Heaton, John (Ricou) Date: 2021.07.27 17:12:51 -04'00'</small></p> <p>Date signed: _____</p>	<p>Bureau Chief Privacy Officer and Co-Authorizing Official Name: Henry J. Holcombe Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-9400 Email: Jamie.Holcombe@uspto.gov</p> <p>I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.</p> <p>Signature: <u>Users, Holcombe, Henry</u> <small>Digitally signed by Users, Holcombe, Henry Date: 2021.07.29 09:54:28 -04'00'</small></p> <p>Date signed: _____</p>
<p>Co-Authorizing Official Name: Andrew Faile Office: Deputy Commissioner for Patent Operations (DCPO) Phone: (571) 272-8800 Email: Andrew.Faile@uspto.gov</p> <p>I certify that this PIA accurately reflects the representations made to me herein by the System Owner, the Chief Information Security Officer, and the Chief Privacy Officer regarding security controls in place to protect PII/BII in this PIA.</p> <p>Signature: <u>Users, Faile, Andrew</u> <small>Digitally signed by Users, Faile, Andrew Date: 2021.07.29 11:40:42 -04'00'</small></p> <p>Date signed: _____</p>	

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.