

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



**Privacy Impact Assessment
for the
Corporate Web Systems (CWS)**

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

09/16/2021

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

Date

U.S. Department of Commerce Privacy Impact Assessment USPTO Corporate Web Systems (CWS)

Unique Project Identifier: PTOI-028-00

Introduction: System Description

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

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

The Corporate Web System (CWS) is an n-tier application architecture that consists of www.uspto.gov, PTOWeb, Reference Document Management Services (RDMS), and Image Gallery. The web servers are responsible for accepting HTTP requests from web clients and passing the requests to the application servers. All hardware components and operating systems supporting the CWS are managed as part of the USPTO Enterprise UNIX Servers (EUS), Service Oriented Infrastructure (SOI), Database Services (DBS) and Network Security Infrastructure (NSI) systems. The CWS provides a feature-rich and stable platform that contains the Organization's Websites that are used at USPTO such as Intranet and USPTO external website.

The subsystems within the CWS System are:

USPTO.GOV (www.uspto.gov) (Internet) provides the public and key stakeholders with information from USPTO about all aspects of intellectual property. It serves as the main web-based information dissemination channel for the Agency and provides links to public-facing, web-based applications used to conduct the Agency's day-to-day operations.

Image Gallery (Image Gallery) provides the ability to catalog, track, and make available a curated set of approved images for use on USPTO web properties. The solution is based on an open source product (Gallery) and is targeted at a limited user group of USPTO internal users.

PTOWeb is the USPTO's corporate intranet website serving as the primary internal communication, information dissemination and collaboration system for employees and contractors. Offices within the USPTO are able to utilize the Intranet Website to meet everyday business goals on the ptoweb.uspto.gov web site.

Reference Document Management Services (RDMS) system is designed to serve as USPTO's enterprise-wide content management solution for the Manual of Patent Examining Procedure (MPEP) and the Trademark Manual of Examining Procedure (TMEP), the primary guidance documents utilized by Patent and Trademark examiners, as well as the Trademark Trial and Appeal Board Manual of Procedure (TBMP), and the Trademark Federal Statutes and Rules (TFSR), a USPTO-created compilation of the rules that is not meant to serve as an official source. The RDMS system allows web-based access to internal and external customers to view these documents.

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

CWS is a major application system.

(b) System location

It is internally hosted at USPTO's Data Center located at 600 Dulany St, 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)

CWS interconnects with the following other systems:

- Enterprise Desktop Platform (EDP)
- Fee Processing Next Generation (FPNG)
- Enterprise Virtual Event Services (EVES)
- Trademark Processing System – External System (TPS- ES)
- Enterprise Monitoring and Security Operations (SCS)
- Enterprise UNIX Servers (EUS)
- Enterprise Windows Servers (EWS)
- OCIO Program Support System (OCIO-PSS)
- Enterprise Record Management and Data Quality System (ERMDQS)
- Network Security Infrastructure (NSI)
- Trademark Processing System – Internal System (TPS-IS)
- Patent Search System – Specialized Search and Retrieval (PSS-SS)
- Patent Capture and Application Processing System – Capture and Initial Processing (PCAPS-IP)
- Patent Capture and Application Processing System – Examination Support (PCAPS-ES)
- Consolidated Financial System (CFS)
- Enterprise Software Services (ESS)
- Information Dissemination Support System (IDSS)
- Database Services (DBS)
- Intellectual Property Leadership Management System (IPLMSS)
- Patent Search System – Primary Search and Retrieval (PSS-PS)
- Enterprise Data Warehouse (EDW)
- Agency Administrative Support System (AASS)
- Data Storage Management System (DSMS)
- Trademark Next Generation (TMNG)
- PBX/VOIP
- Patent End to End (PE2E)

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

www.uspto.gov

www.uspto.gov (Internet) provides the public and key stakeholders with information from USPTO about all aspects of intellectual property. It serves as the main web-based information dissemination channel for the Agency and provides links to public-facing, web-based applications used to conduct the Agency's day-to-day operations.

Image Gallery

The Image Gallery provides the ability to catalog, track, and make available a curated set of approved images for use on USPTO web properties. The solution is based on an open source product (Gallery) and is targeted at a limited user group of USPTO internal users.

PTOWeb

PTOWeb is the USPTO's corporate intranet website serving as the primary internal communication, information dissemination and collaboration system for employees and contractors. Offices within the USPTO are able to utilize the Intranet Website to meet everyday business goals on the ptoweb.uspto.gov web site.

RDMS

The Reference Document Management Services (RDMS) system is designed to serve as USPTO's enterprise-wide content management solution for the Manual of Patent Examining Procedure (MPEP) and the Trademark Manual of Examining Procedure (TMEP), the primary guidance documents utilized by Patent and Trademark examiners, as well as the Trademark Trial and Appeal Board Manual of Procedure (TBMP), and the Trademark Federal Statutes and Rules (TFSR), a USPTO-created compilation of the rules that is not meant to serve as an official source. The RDMS system allows web-based access to internal and external customers to view these documents.

(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 CWS via the internet and internal USPTO network.

(g) Any information sharing conducted by the system

The www.uspto.gov component, as the main, web-based information dissemination channel for the Agency publishes public PII in the form of senior leadership biographies and news stories about interesting people in the world of Intellectual Property.

The ptoweb.uspto.gov component similarly publishes senior leader's biographies and also some business unit contacts (name and contact information). The Image Gallery component publishes some staff names and photos (typically senior staff).

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

35 U.S.C. 2 and OCIO's mission to disseminate public patent and trademark information. The www.uspto.gov component is one mechanism the Agency uses to fulfill its constitutional requirement to promote the progress of science and useful arts.

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

CWS is a Moderate system.

Section 1: Status of the Information System

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

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

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

- This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.
- This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or 01-2017).
- This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2019 or later).

Section 2: Information in the System

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

Identifying Numbers (IN)					
a. Social Security*	<input type="checkbox"/>	f. Driver's License	<input type="checkbox"/>	j. Financial Account	<input type="checkbox"/>
b. Taxpayer ID	<input type="checkbox"/>	g. Passport	<input type="checkbox"/>	k. Financial Transaction	<input type="checkbox"/>
c. Employer ID	<input type="checkbox"/>	h. Alien Registration	<input type="checkbox"/>	l. Vehicle Identifier	<input type="checkbox"/>
d. Employee ID	<input type="checkbox"/>	i. Credit Card	<input type="checkbox"/>	m. Medical Record	<input type="checkbox"/>

e. File/Case ID	<input type="checkbox"/>			
n. Other identifying numbers (specify):				
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:				

General Personal Data (GPD)					
a. Name	<input checked="" type="checkbox"/>	h. Date of Birth	<input type="checkbox"/>	o. Financial Information	<input type="checkbox"/>
b. Maiden Name	<input type="checkbox"/>	i. Place of Birth	<input type="checkbox"/>	p. Medical Information	<input type="checkbox"/>
c. Alias	<input type="checkbox"/>	j. Home Address	<input type="checkbox"/>	q. Military Service	<input checked="" 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 checked="" type="checkbox"/>	t. Mother's Maiden Name	<input type="checkbox"/>
g. Citizenship	<input type="checkbox"/>	n. Religion	<input type="checkbox"/>		
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	<input checked="" type="checkbox"/>	e. Work Email Address	<input checked="" type="checkbox"/>	i. Business Associates	<input checked="" 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 checked="" 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 checked="" 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 checked="" type="checkbox"/>	h. Eye Color	<input type="checkbox"/>	m. DNA Sample or Profile	<input type="checkbox"/>
d. Video Recording	<input checked="" type="checkbox"/>	i. Height	<input type="checkbox"/>	n. Retina/Iris Scans	<input type="checkbox"/>
e. Photographs	<input checked="" type="checkbox"/>	j. Weight	<input type="checkbox"/>	o. Dental Profile	<input type="checkbox"/>
p. Other distinguishing features/biometrics (specify):					

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

Other Information (specify)

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

Directly from Individual about Whom the Information Pertains					
In Person	<input checked="" type="checkbox"/>	Hard Copy: Mail/Fax	<input type="checkbox"/>	Online	<input checked="" type="checkbox"/>
Telephone	<input checked="" type="checkbox"/>	Email	<input checked="" 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 checked="" type="checkbox"/>	Private Sector	<input checked="" type="checkbox"/>	Commercial Data Brokers	<input type="checkbox"/>
Third Party Website or Application			<input checked="" type="checkbox"/>		
Other(specify):					

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

<p>The information is provided by the individual directly and USPTO ensures that the non-sensitive Personally Identifiable Information in CWS is secured using appropriate administrative, physical, and technical safeguards in accordance with the federal policies. All access has role-based restrictions, and individuals with access privileges have undergone vetting and suitability screening. The USPTO maintains an audit trail and performs random periodic reviews to identify unauthorized access and changes as part of verifying the integrity of data.</p>

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. OMB 0690-0035 OMB 0651-0077</p>
<input type="checkbox"/>	<p>No, the information is not covered by the Paperwork Reduction Act.</p>

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 checked="" type="checkbox"/>
For administrative matters	<input checked="" type="checkbox"/>	To promote information sharing initiatives	<input checked="" type="checkbox"/>
For litigation	<input type="checkbox"/>	For criminal law enforcement activities	<input type="checkbox"/>
For civil enforcement activities	<input type="checkbox"/>	For intelligence activities	<input type="checkbox"/>
To improve Federal services online	<input checked="" type="checkbox"/>	For employee or customer satisfaction	<input checked="" 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 information in this system is about DOC employees and members of the public. The CWS provides a feature-rich and stable platform that contains the Organization's Websites that are used at USPTO such as Intranet and USPTO external website.

Senior leadership biography examples are located here: <https://www.uspto.gov/about-us/executive-biographies>

News worthy innovator examples are located here: <https://www.uspto.gov/learning-and-resources/journeys-innovation>

All content on www.uspto.gov is reviewed and approved as per [AAO219](#) and related handbooks.

On PTOWeb, there are similar senior leadership biographies and most business units list contact information.

Image Gallery is a repository to hold photos of leadership that are approved for use internally.

- 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.)

Adversarial entities, foreign governments, insider threats and inadvertent private information exposure are all risks and USPTO has policies, procedures and training to ensure that employees are aware of their responsibility of protecting sensitive information and the negative impact on 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 current USPTO 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), USPTO Rules of the Road (OCIO-POL-36). All offices of the USPTO adhere to the USPTO Records Management Office's Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citation.

Section 6: Information Sharing and Access

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

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" 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 checked="" type="checkbox"/>
Private sector	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign governments	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign entities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other(specify):	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The PII/BII in the system will not be shared.

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

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

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

<input checked="" type="checkbox"/>	<p>Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:</p> <p>CWS interconnects with the following other systems:</p> <ul style="list-style-type: none"> • Fee Processing Next Generation (FPNG) • Enterprise Virtual Event Services (EVES) • Trademark Processing System– External System (TPS-ES) • Enterprise Monitoring and Security Operations (SCS) • Trademark Processing System– Internal System (TPS-IS) • Patent Search System– Specialized Search and Retrieval (PSS-SS) • Patent Capture and Application Processing System– Capture and Initial Processing (PCAPS-IP) • Patent Capture and Application Processing System– Examination Support (PCAPS-ES) • Consolidated Financial System (CFS)
-------------------------------------	--

	<ul style="list-style-type: none"> • Enterprise Software Services (ESS) • Information Dissemination Support System (IDSS) • Intellectual Property Leadership Management System (IPLMSS) • Patent Search System – Primary Search and Retrieval (PSS-PS) • Agency Administrative Support System (AASS) • Data Storage Management System (DSMS) • Trademark Next Generation (TMNG) • PBX/VOIP • Patent End to End (PE2E) <p>All data transmissions are encrypted and require credential verification. All data transmissions not done through dedicated lines require security certificates. Inbound transmissions as well as outbound transmissions to government agencies pass through a DMZ before being sent to endpoint server. USPTO requires annual security role-based training and annual mandatory security awareness procedure training for all employees. The following are current USPTO 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), USPTO Rules of the Road (OCIO-POL- 36). All offices of the USPTO adhere to the USPTO Records Management Office's Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citation.</p>
<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 checked="" 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 checked="" type="checkbox"/>	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: News worthy innovators may decline to be featured. Anyone can request their information be removed from PTOWeb by talking to their business unit supervisor. Image Gallery can administratively delete any photograph if asked to be removed.
<input type="checkbox"/>	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

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

<input checked="" type="checkbox"/>	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: News worthy innovators sign a consent as part of the process of creating the article.
<input type="checkbox"/>	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

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

<input checked="" type="checkbox"/>	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Senior leaders can request updates to their bios; news worthy innovator can provide corrections to fact. Employees can request their information be taken down from PTOWeb, as well as Image Gallery.
<input type="checkbox"/>	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.)

<input type="checkbox"/>	All users signed a confidentiality agreement or non-disclosure agreement.
<input 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 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: As with all content on the websites, access is logged both in server logs and, for www.uspto.gov and ptoweb.uspto.gov with Google Analytics.
<input checked="" type="checkbox"/>	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): <u> 1/28/2021 </u> <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
<input checked="" type="checkbox"/>	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a

	moderate or higher.
<input checked="" type="checkbox"/>	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
<input checked="" type="checkbox"/>	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
<input checked="" type="checkbox"/>	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
<input type="checkbox"/>	Contracts with customers establish DOC ownership rights over data including PII/BII.
<input type="checkbox"/>	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
<input type="checkbox"/>	Other (specify):

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

In general, author accounts are limited to trained authors, administrative accounts follow least privilege principles, and web communication is encrypted via https. Personally Identifiable Information (PII) in CWS is secured using appropriate administrative, physical, and technical safeguards in accordance with the applicable federal laws, executive orders, directives, policies, regulations, and standards. All access has role based restrictions, and individuals with access privileges have undergone vetting and suitability screening. Data is maintained in areas accessible only to authorized personnel. The USPTO maintains an audit trail and performs random periodic reviews to identify unauthorized access. Additionally, systems are secured by various USPTO infrastructure components, including the Network and Security Infrastructure (NSI) system and other OCIO established technical controls to include password authentication at the server and database levels.

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> Biographical Files and Social Networks- COMMERCE/DEPT-20 Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs. – COMMERCE/DEPT-23 Dissemination Events and Registrations. – COMMERCE/ PAT-TM-19
<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: GRS 5.1, item 020 N1-241-06-2:1; Trademarks Program and Policy Subject Files N1-241-10-1:1b; Patent Program and Policy Subject Files
<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 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 checked="" 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 type="checkbox"/>	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
<input type="checkbox"/>	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

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

<input checked="" type="checkbox"/>	Identifiability	Provide explanation: Name, telephone number, email address can be used to identify an individual.
<input checked="" type="checkbox"/>	Quantity of PII	Provide explanation: The PII is publicly available and varies

		based upon request.
<input checked="" type="checkbox"/>	Data Field Sensitivity	Provide explanation: PII published on the www.uspto.gov component is public information. PTOWeb and Image Gallery are only internally accessed.
<input checked="" type="checkbox"/>	Context of Use	Provide explanation: Senior leaders and newsworthy innovators provide their public PII to USPTO's Office of Chief Communications officer for bios and news stories typically via email for use on uspto.gov and PTOWeb.
<input checked="" type="checkbox"/>	Obligation to Protect Confidentiality	Provide explanation: This system is governed by The Privacy Act of 1974, which prohibits the disclosure of information from a system of records absent of the written consent of the subject individual.
<input checked="" type="checkbox"/>	Access to and Location of PII	Provide explanation: It is publically accessed and public information on www.uspto.gov. PTOWeb and Image Gallery are only internally accessed.
<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.)

Insider threats and adversarial entities are the potential threat to the information system. Each bio or article published on the www.uspto.gov website is completely reviewed before publishing. We do not publish any sensitive PII on any components of the CWS. Personally Identifiable Information (PII) in CWS is secured using appropriate administrative, physical, and technical safeguards in accordance with the applicable federal laws, executive orders, directives, policies, regulations, and standards.

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.