Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
MyUSPTO Cloud (MyUSPTO-C)

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: 2024.06.06 13:31:30 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment USPTO MyUSPTO Cloud (MyUSPTO-C)

Unique Project Identifier: PTOC-054-00

Introduction: System Description

Provide a brief description of the information system.

MyUSPTO Cloud (MyUSPTO-C) is a web site for United States Patent and Trademark Office (USPTO) employees, contractors, and members of the public to track patent applications and grants, check trademark registrations and statuses, and to actively manage their intellectual property portfolio within a personalized gateway. The system also allows a limited number of USPTO employees to upload court notification documents to the appropriate Patent and Trademark Systems.

The MyUSPTO-C system also offers a component for the USPTO legal team. This feature, The Court Notice Processing System (CNPS), allows members of the USPTO Legal team to process United States (US) Courts notice documents for lawsuits that involve patents and trademarks into Patent's EventHub, and Trademark's Trademark Next Generation-Content Management System (TMNG-CMS) and Prosecution History systems. CNPS is located on MyUSPTO-C's Administration and Operations internal web site. It is restricted via role-based-access control ICAM Identity as a Service (ICAM-IDaaS) to a limited number of designated legal team users. CNPS resides in the Amazon Web Services (AWS) cloud within the MyUSPTO infrastructure.

Address the following elements:

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

(b) System location
MyUSPTO-C is located on a cloud-based platform hosted by AWS US East Northern Virginia (VA).

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
MyUSPTO-C interconnects with the following systems:

- **Enterprise Software Services (ESS)** is comprised of multiple on premise and in the cloud software services, which support the USPTO in carrying out its daily tasks. Within this system, the services are broken up into several subsystems. These include but are not limited to Enterprise Active Directory Services (EDS), Email as a Service

(EaaS), Enterprise SharePoint Services (ESPS).

•**Security and Compliance Services (SCS)** is a general support system comprised of subsystems, and provides enterprise-level monitoring to the USPTO.

•**Network and Security Infrastructure System (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 USPTO Information Technology (IT) applications.

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

•**Fee Processing Next Generation (FPNG)** is a major application, and provides fee processing solutions within USPTO. FPNG replaced the Revenue Accounting and Management (RAM) system, which served as a subsidiary to the core financial system, Momentum.

•**Data Delivery System (DDS)** provides services containing reference data to all business units. The most recognizable reference data managed within the component are the State, Country and Geographic Region codes.

•**Information Dissemination Support System (IDSS)** is comprised of several subsystems that provide automated support for the timely search and retrieval of electronic text and images concerning patent applications and patents by USPTO internal and external users. Among the several subsystems ae Assignments Historical Data (AHD), Assignments on the Web (AOTW), Certified Copy Center (CCC), and Intellectual Property Assignment Systems (IPAS).

•**Trademark Trial and Appeal Board Center (TTAB)** is a system that provides intake and exam centers for Administrative Judges, Interlocutory Attorneys, and Professional Staff.

•**Trademark Next Generation (TMNG)** is a major system providing support for the automated processing of trademark applications for the USPTO. TMNG features the ability to interface with related systems within USPTO. One such subsystem is TMNG-CMS.

•**Patent End to End (PE2E)** is a major application, and provides examination tools used for the examination, issuance, and granting of patents. A component under this major is Patent Center.

•**Patent Business Content Management Services (PBCMS)** consists of several components that allow users to access patent application documents and content stored in various formats. One such component is Event-Hub.

(d) *The way the system operates to achieve the purpose(s) identified in Section 4*
Users' access MyUSPTO-C via the URL https://my.uspto.gov/. At the home page of MyUSPTO.gov, users can create a new account with information such as an email address, first name, last name, and phone number or log into an existing account, with an email address, password and a required form of MFA. Once logged into the site, users manage their intellectual property portfolio within a personalized gateway.

(e) *How information in the system is retrieved by the user*
Users enter their username, password and MFA credentials to gain access to their personalized USPTO Business Gateway. The personalized gateway is composed of widgets. Widgets consist of links to various USPTO backend services. Patent and Trademark docket widgets allow users to create collections containing applications, registered trademarks, and patents that they can track, share, and monitor. Notifications on docket widgets provide status updates and recent status changes. For example, within the Trademark Form Finder widget, users click on the File application link. The link will open to the Trademark Electronic Application System (TEAS) to complete and file an application.

(f) *How information is transmitted to and from the system*
USPTO follows strict guidelines regarding handling and transmitting PII/BII. Data transmitted to and from MyUSPTO-C is protected by secure methodologies such as Hypertext Transfer Protocol Secure (HTTPS), used for secure communication over a computer network and Internet. In HTTPS, the communication protocol is encryption using Transport Layer Security 1.2 (TLS 1.2). Security Assertion Markup Language 2.0 (SAML 2.0) is used for exchanging authentication and authorization identities between security domains. All data stored at rest is also encrypted.

(g) *Any information sharing*
Information may be shared on a case-by-case basis and via bulk transfer within the bureau.

(h) *The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information*
The following federal laws provide the specific programmatic authority for collecting, maintaining, using, and disseminating the information: 5 U.S.C. 301, 5 U.S.C. 552, 35 U.S.C. 2, 35 U.S.C. 41, and 44 U.S.C. 3101.

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

MyUSPTO-C 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	☐	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): serial number related to a particular patent or trademark.					
*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):					

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.

The accuracy of the information within MyUSPTO-C is ensured by obtaining the information directly from the individual for which the information pertains. The individual is also able to view their information within MyUSPTO-C and either update it themselves or notify USPTO if there is an error.

MyUSPTO-C is secured using appropriate administrative, physical and technical safeguards in accordance with the National Institute of Standards and Technology (NIST) security controls (encryption, access control, auditing). Mandatory IT Awareness and role-based training is required for staff who have access to the system and addresses how to handle, retain, and dispose of data. 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.

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.

☒	No, the information is not covered by the Paperwork Reduction Act.

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

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards	☐	Biometrics	☐
Caller-ID	☐	Personal Identity Verification (PIV) Cards	☐
Other (specify):			

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

Section 3: System Supported Activities

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

Activities			
Audio recordings	☐	Building entry readers	☐
Video surveillance	☐	Electronic purchase transactions	☐
Other (specify):			

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

Section 4: Purpose of the System

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

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

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).

MyUSPTO-C collects information about USPTO employees, contractors and members of the public for administrative matters, to improve federal services online, for employee and customer satisfaction, and for web measurement and customization technologies (multi-session). MyUSPTO-C provides users with the online convenience of conducting official patent and trademark business and corresponding with USPTO representative via the site. PII is collected to identify the users of the system when authenticating through the network. User credentials are managed through ICAM-IDaaS/Okta, which provides authentication and authorization of user access. This allows users to access USPTO's network and various systems through Single Sign-On (SSO). Also, the collected information is intended to be used by the USPTO Service Desk for verifying the identity of customers interacting with MyUSPTO-C. If a customer forgets the password to their MyUSPTO account, PII collected would be used to verify the customer. MyUSPTO-C gives users customization options, such as notifications and search. Users are provided with multi-session capabilities, where they are able to have three or four applications open at a time and are able to log in multiple times and still be remembered.

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.)

MyUSPTO-C implements security and management controls to prevent the inappropriate disclosure of sensitive information. Automated mechanisms are in place to ensure the security of all data collected. Security controls are employed to ensure information is resistant to tampering (Physical and Access Controls), the confidentiality of data in transit (Encryption), and that data is available for authorized users only (Access Control). Management controls are utilized to prevent the inappropriate disclosure of sensitive information. In addition, the NSI and SCS provide additional automated transmission and monitoring mechanisms to ensure that PII is protected and not breached by any outside entities.

USPTO has also identified and evaluated potential threats to PII such as insider threats and adversarial entities which may cause a loss of confidentiality, accessibility and integrity of information. Users are provided one-on-one, weekly, and monthly training. All users have access restriction or permissions based on the built-in security controls of the system. Furthermore, the system has the ability to password protect any sensitive data for added protection. System access to PII/BII data is limited to a restricted set of users.

The security safeguards for MyUSPTO-C shall meet the NIST SP 80-53 (Rev. 5) requirements set forth in the System Security and Privacy Plan (SSPP), the USPTO Cybersecurity Baseline Policy, and all higher directives. All systems are subject to monitoring that is consistent with applicable regulations, agency policies, procedures, and guidelines. MyUSPTO-C is continually monitored to provide "near real-time" risk reporting and mitigation activities. MyUSPTO-C has put certain security controls 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. 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	☒	☒	☒
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: •SCS •FPNG •PE2E •ICAM-IDaaS •ESS •PBCMS •PE2E •TTAB •TMNG •IDSS The security safeguards for MyUSPTO-C shall meet the NIST SP 80-53 (Rev. 5) requirements set forth in the System Security and Privacy Plan (SSPP), the USPTO Cybersecurity Baseline Policy, and all higher directives. All systems are subject to monitoring that is consistent with applicable regulations, agency policies, procedures, and guidelines. MyUSPTO-C is continually monitored to provide "near real-time" risk reporting and mitigation activities. MyUSPTO-C has put certain security controls 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. 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.
☐	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: Through this PIA
□	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: USPTO employees and contractors use SSO through ICAM-IDaaS and the PII/BII is necessary to obtain access to the system. MyUSPTO-C collects no PII/BII about an individual when visiting the site unless the individual is creating a user account. Members of the public that require log-in access to the system do not have the opportunity to decline to provide PII/BII as the information is required for the purpose and access of the system.

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: Yes, members of the public have an opportunity to consent to particular uses of their PII/BII. Submitting personal information is voluntary. When a user voluntarily submits information, it constitutes their consent to use the information for purposes stated at the time of collection.
☒	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: USPTO employees and contractors use SSO through ICAM-IDaaS and so do not have an opportunity to consent to particular uses of PII. Members of the public that require log-in account access do not have the opportunity to consent to particular uses of their PII/BII, as the information collected is necessary for the purpose of the system.

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: Yes, individuals have an opportunity to review/update PII/BII pertaining to them. Public users may access the patent or trademark assistance center to request an update to their record. USPTO employees and contractors may update their information via the human resources department.
☐	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: Audit logs.
☒	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): 11/22/2024 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
☒	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
☒	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 5 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).*

PII in MyUSPTO-C 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 authorize personnel. The USPTO maintains an audit trail and performs random periodic reviews to identify unauthorized access. Additionally, My-USPTOC is secured by various USPTO infrastructure components, including the NSI system and other OCIO established technical controls that includes end-to-end transport layer protocols and where applicable data-at-rest and in-transit encryption.

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-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: •GRS 3.2: Information Systems Security Records, Item 030 - System Access Rec •GRS 5.2, Transitory and Intermediary Records, Item 010 - Transitory Records
☐	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
☒	Yes, retention is monitored for compliance to the schedule.
☐	No, retention is not monitored for compliance to the schedule. Provide explanation:

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

Disposal			
Shredding	☐	Overwriting	☒
Degaussing	☐	Deleting	☒
Other (specify):			

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

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

☒	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
☐	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
☐	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

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

☒	Identifiability	Provide explanation: MyUSPTO-C collects, maintains, or disseminates PII about members of the public. The type of information includes email address, first name, last name, physical address and phone number. When combined, this data set can uniquely identify an individual.
☒	Quantity of PII	Provide explanation: The quantity of PII is based several factors but the primary driver of the large amount of data will be based on the number of users accessing and creating an account on the site and the quantity of patent and trademark data.
☒	Data Field Sensitivity	Provide explanation: The combination of email address, first name, last name, phone number do not make the data more sensitive because the information is publicly available.
☒	Context of Use	Provide explanation: The email address, first name, last name, and phone number collected will be used primarily for account creation and logging into the system.
☒	Obligation to Protect Confidentiality	Provide explanation: USPTO Privacy Policy requires the PII information collected within the system to be protected accordance to NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information. In accordance with the Privacy Act of 1974, PII must be protected.
☒	Access to and Location of PII	Provide explanation: Access to MyUSPTO-C is limited to authorized personnel only, government personnel, and contractors.
☐	Other:	Provide explanation:

<u>Section 12</u>: 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.)

Foreign and adversarial entities, insider threats, and computer failure may raise privacy concerns related to the collection, maintenance, and dissemination of PII. To mitigate this risk. System users undergo annual mandatory training regarding appropriate handling of information. Physical servers storing the potential PII are located in a highly sensitive zone within the cloud and logical access is segregated with network firewalls and switches through an Access Control list that limits access to only a few approved and authorized accounts. USPTO monitors, in real-time, all activities and events within the servers storing the potential PII data and personnel review audit logs received on a regular bases and alert the appropriate personnel when inappropriate or unusual activity is identified.

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.