Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
Trademark Trial and Appeal Board Center (TTABC)

Reviewed by: Deborah Stephens, 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

NICHOLAS CORMIER Digitally signed by NICHOLAS CORMIER
Date: 2025.09.10 12:03:56 -04'00' 9/10/2025

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO Trademark Trial and Appeal Board Center (TTABC)

Unique Project Identifier: TPL-TTAB-01-00

Introduction: System Description

Provide a brief description of the information system.

The Trademark Trial and Appeal Board Center (TTABC) master system boundary consists of two components: Trademark Trial and Appeal Board - Center (TTAB-C) and Trademark Trial and Appeal Board Reading Room (TTABRR).

TTAB-C is the administrative tribunal within the United States Patent and Trademark Office (USPTO) that processes trademark appeals, oppositions, cancellations, and concurrent use proceedings. TTAB-C public customers can complete and submit trademark forms electronically via a web interface. The submissions are transferred to the TTAB group for normal intake processing and all proceedings are brought before the board. The board can generate actions, track the status of proceedings, record data, and issue reports.

TTABRR allows for the electronic identification and handling of TTAB final decision documents. These documents are required to be publicly available in accordance with the Freedom of Information Act.

Address the following elements:

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

TTABC is a major application.

(b) System location

TTABC is located within Amazon Web Services US East in Ashburn, Virginia.

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

TTABC interconnects with:

Enterprise Software Services (ESS): provides the United States Patent and trademark Office (USPTO) organization with a collection of programs that utilize common business applications and tools for modeling how the entire organization works. In addition, ESS provides a

centralized solution for assisting developers in building applications unique to the organization. The software implemented is intended to solve an enterprise-wide problem, rather than specific departmental issues. Enterprise level software aims to improve the enterprise's productivity and efficiency by providing business logic and support functionality, continuous collaborative and communication tools for organizational personnel to complete their everyday task.

USPTO Amazon Cloud Services (UACS): The UACS Infrastructure-as-a-Service (IaaS) platform is used to support USPTO information systems hosted in the Amazon Web Services (AWS) East/West environment. UACS leverages AWS Infrastructure as a Service (IaaS) mode that enables on-demand internet access to a shared pool of configurable computing resources including servers, storage, network infrastructure, and other web-based services.

Fee Processing Next Generation (FPNG): USPTO's "Next Gen" solution for fee processing. FPNG allows internal and external users to manipulate payment accounts, perform profile updates, and make payments for USPTO goods and services.

Intellectual Property Leadership Management Support System (IPLMSS): is a Major Application that facilitates grouping and management of separate information system boundaries that collectively support the USPTO Director, Deputy Director, Office of the General Counsel (OGC), Office of the Solicitor, Office of Enrollment and Discipline (OED), Trademark Trial and Appeal Board (TTAB), Patent Trial and Appeal Board (P-TACTS); Office of Patent Training (OPT); and Office of Policy and International Affairs (OPIA).

MyUSPTO Cloud (MyUSPTO-C): A web site for 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.

Trademark Next Generation (TMNG): is an information system that provides support for the automated processing of trademark applications for the USPTO. TTABC connects with Trademark Common Data Services (TMCOM), which resides within the TMNG system boundary.

ICAM Identity as a Service (ICAM-IDaaS): is an Okta Identity cloud infrastructure is Identity as a Service built and maintained by Okta (the system is FedRAMP and hosted on AWS Cloud) as a true cloud-native service. As an identity service it provides Universal Directory, Single Sign-On, Lifecycle Management and Adaptive Multi-Factor Authentication. This service processes Personally Identifiable Information (PII) data.

Network and Security Infrastructure System (NSI): NSI helps with the network connections for TTABC.

Interconnections to assist with Security Management:

Crowdstrike: USPTO tool that is utilized to update and monitory configuration changes on the TTABC servers.

Security and Compliance Services (SCS): USPTO Security tool that is utilized to audit, scan, and monitor security relevant events.

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

TTABC accomplishes its purpose through a web application that a user (or their lawyer) wishing to file proceedings. The user must first log into MyUSPTO. The web application presents the user with pages to fill out about their trademark (or unregistered mark). After filling out all the pages and paying the associated fees through FPNG, proceedings are submitted for processing. The submissions are transferred to the TTAB group for normal intake processing and all proceedings are brought before the board.

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

All interaction from the user is through the web interface.

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

Information is transmitted from the user via the web interface. The system interacts with other systems via application programming interfaces (APIs) and Extensible Markup Language (XML) documents.

(g) Any information sharing

Information will be shared with the public.

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

5 U.S.C. 552, 35 U.S.C. 2;
37 CFR Part 2 – Rules of Practice in Trademark Cases;
15 U.S.C. Section 1051 et sec. (Lanham Act);
Madrid Protocol

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

Moderate

Section 1: Status of the Information System

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

☐ This is a new information system.

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

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

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

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

Section 2: Information in the System

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

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

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

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

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

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

Other Information (specify)

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

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

Government Sources					
Within the Bureau	☒	Other DOC Bureaus	☐	Other Federal Agencies	☒
State, Local, Tribal	☐	Foreign	☐		
Other (specify):					

Non-government Sources					
Public Organizations	☒	Private Sector	☒	Commercial Data Brokers	☐
Third Party Website or Application			☐		
Other (specify):					

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

The accuracy of the information is ensured by the users directly providing the information and having the responsibility to review/update their information within their MyUSPTO account. They can also directly update it within TTAB Center for the specific information displayed on the page.

The system is secured using appropriate administrative, physical, and technical safeguards in accordance with the National Institute of Standards and Technology (NIST) and Federal Risk and Authorization Management (FedRAMP) security controls (encryption, access control, and auditing). Mandatory information technology (IT) awareness and role-based training is required for staff who have access to the system and address how to handle, retain, and dispose of data. All access has role-based restrictions and individuals with privileges have undergone vetting and suitability screen. The USPTO maintains an audit trail and performs random, periodic reviews (quarterly) to identify unauthorized access and changes as part of verifying the integrity of administrative account holder data and roles.

2.4 Is the information covered by the Paperwork Reduction Act?

☒	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.

	0651-0040, Trademark Trial and Appeal Board (TTAB) Actions PTO2120_Notice of Opposition
☐	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): Click or tap here to enter text.			

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

Section 4: Purpose of the System

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

Purpose			
For a Computer Matching Program	☐	For administering human resources programs	☐
For administrative matters	☐	To promote information sharing initiatives	☐
For litigation	☒	For criminal law enforcement activities	☐
For civil enforcement activities	☐	For intelligence activities	☐
To improve Federal services online	☒	For employee or customer satisfaction	☐

For web measurement and customization technologies (single-session)	☐	For web measurement and customization technologies (multi-session)	☐
Other (specify):			

Section 5: Use of the Information

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

PII is used to authenticate users to the system and associates public users and their representatives with their filings. PII is used during the TTAB process as required for litigation. Bar membership is used to verify attorney is a practicing member of the bar in good standing.

USPTO employees, contractors, other federal agency representatives, and members of the public have access to the system to perform duties before the TTAB and improves federal services online.

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.)

In the event of computer failure, insider threats, or attack against the system by adversarial or foreign entities, any potential PII data stored within the system could be exposed or corrupted. To avoid a breach, the system has certain security controls in place to ensure that information is handled, retained, and disposed of appropriately. Access to individual's PII is controlled through the application. All personnel who access the data must provide authentication to access the system. An audit trail is generated when the database is accessed. These audit trails are based on application server out-of-the-box logging reports reviewed by the Information System Security Officer (ISSO) and System Auditor. Any suspicious indicators are immediately investigated and appropriate action is taken, if necessary. System users undergo annual mandatory training regarding appropriate handling of information."

All data transmissions are encrypted and requires credential verification. All data transmissions not done through dedicated lines require security certificates. Inbound transmissions as well as outbound transmissions pass through a DMZ before being sent to endpoint servers. Access controls, auditing and encryption are leveraged to prevent PII/BII leakage. In accordance with the USPTO Privacy Policy guidelines, all systems that process PII and have interconnections are designed and administered to ensure the confidentiality of PII provided to and by TTAB-C.

Specific safeguards that are employed by the systems:
• The systems and its facility are physically secured and closely monitored. Only individuals authorized by USPTO are granted logical access to the system.
• Technical, operational, and management security controls are in place and are verified regularly.
• Periodic security testing are conducted on the systems to help detect new security vulnerabilities on time.
• All personnel are trained to securely handle PII information and to understand their responsibilities for protecting PII.

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): Plaintiff (only for TTAB-C component)	☒	☐	☐

☐	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: FPNG IPLMSS MyUSPTO-C PS-CC ICAM IDaaS ESS UACS NSI CISO-CC Crowdstrike SCS TMNG All data transmissions are encrypted and requires credential verification. All data transmissions not done through dedicated lines require security certificates. Inbound transmissions as well as outbound transmissions pass through a DMZ before being sent to endpoint servers. Access controls, auditing and encryption are leveraged to prevent PII/BII leakage. In accordance with the USPTO Privacy Policy guidelines, all systems that process PII and have interconnections are designed and administered to ensure the confidentiality of PII provided to and by TTABC. Specific safeguards that are employed by the systems: • The systems and its facility are physically secured and closely monitored. Only individuals authorized by USPTO are granted logical access to the system. • Technical, operational, and management security controls are in place and are verified regularly. • Periodic security testing are conducted on the systems to help detect new security vulnerabilities on time. • All personnel are trained to securely handle PII information and to understand their responsibilities for protecting PII.
☐	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 policy. The privacy policy can be found at: https://www.uspto.gov/privacy-policy	
☐	Yes, notice is provided by other means.	Specify how:
☐	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: For cases to be filed and adjudicated, the individuals involved with the case must be identified. The submitter of the documentation can limit what information is provided upon filing; however, in order to proceed, a minimum threshold of PII must be submitted.

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

☐	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
☒	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: PII is required as part of the TTAB process. In specific and rare cases, upon conclusion of the filing of the notice of opposition, requester may petition USPTO to redact information.

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: Users are responsible for reviewing and updating the information within their USPTO account. They can also update limited information directly through the TTAB center.
☐	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): 10/7/2024 ☐ 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 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 within the system is secured using appropriate management, operational, and technical safeguards in accordance with NIST and FedRAMP requirements. Such management controls include the review process to ensure that management controls are in place and documented in the System Security Privacy Plan (SSPP). The SSPP specifically addresses the management, operational, and technical controls that are in place and planned during the operation of the system. Operational safeguards include restricting access to PII data to a small subset of users. 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 system maintains an audit trail and the appropriate personnel is alerted when there is suspicious activity. Data is encrypted in transit and at rest.

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 Commerce/PAT-TM-26 Trademark Application and Registration 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.)*

General Records Schedules (GRS) | National Archives

☒	There is an approved record control schedule. Provide the name of the record control schedule: N1-241-06-2:4, Trademark Case File Feeder Records and Related Indexes
☐	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: The system includes submitter's name, address, phone number, and other identifiers that can be used to identify an individual.
☒	Quantity of PII	Provide explanation: These numbers may vary based on how many applications are received but is in the thousands.
☒	Data Field Sensitivity	Provide explanation: Data fields include name, home address, home telephone number, home email address, file/case number, and bar membership number.
☒	Context of Use	Provide explanation: TTAB Center is used for litigation purposes as part of the TTAB process.
☒	Obligation to Protect Confidentiality	Provide explanation: NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 5 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); and

		the Privacy Act of 1974.
☒	Access to and Location of PII	Provide explanation: PII is contained in UACS in Ashburn, Virginia.
☒	Other:	Provide explanation: While the loss of confidentiality, integrity, or availability would be adverse, it would not prevent the system mission from continuing and therefore would not be catastrophic.

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.)

System users undergo annual mandatory training regarding appropriate handling of information. Access to servers is restricted to only a few authorized individuals. The servers storing the potential PII are located in a highly sensitive zones 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 an authorized account. 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.