Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
Trademark Processing System – Internal Systems (TPS-IS)

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

CHARLES CUTSHALL Digitally signed by CHARLES CUTSHALL
Date: 2025.05.06 11:13:29 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO Trademark Processing System – Internal Systems (TPS-IS)

Unique Project Identifier: PTOT-003-00

Introduction: System Description

Provide a brief description of the information system.

The Trademark Processing System – Internal Systems (TPS-IS) is an information system that provides support for the automated processing of trademark applications for the United States Patent and Trademark Office (USPTO). TPS-IS features the ability to interface with related systems within USPTO. TPS-IS has established new system interconnections with the migration from the legacy system to the cloud base technology for seamless utilization. TPS-IS includes four applications that are used to support USPTO staff through the trademark review process. The four applications are listed below:

First Action System for Trademarks 2 - FAST2
Trademark Cropped Image Manager - TCIM
Trademark Image Capture and Retrieval System - TICRS
Trademark Data Entry and Update System - TRADEUPS

Address the following elements:

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

TPS-IS is a major application.

(b) System location

TPS-IS is located at Alexandria, Virginia.

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

TPS-IS interconnects with:

Trademark Processing System (External) (TPS-ES) - is a major application that provides customer support for processing Trademark applications for USPTO. TPS-ES includes applications used to support USPTO staff and public users through the trademark application process.

Trademark Next Generation (TMNG) - is a major application and provides support for the automated processing of trademark applications for the USPTO.

Intellectual Property Leadership Management Support System (IPLMSS) - is a major Application information system, which provides, which provides various capabilities and functionality for the USPTO.

Information Dissemination Support System (IDSS) - provides automated support for the timely search and retrieval of electronic text and images concerning patent applications and patents by USPTO internal and external users.

Storage and Infrastructure Managed Service (SIMS) - is responsible for the implementation of encryption of data at rest for the USPTO.

Madrid International Trademark System (MITS) - assists the Office of Trademark in sending, receiving, reviewing and verifying data from International Bureau (IB)-related to international applications that are being handled by the USPTO as governed by the Madrid Protocol.

Network and Security Infrastructure (NSI) - facilitates the communications, secure access, and network infrastructure support for all USPTO applications.

Database Services (DBS) - provides performance monitoring for enterprise and product owned MYSQL and Oracle databases.

Security and Compliance Services (SCS) - is an application which provide enterprise-wide security capability for all USPTO systems. systems.

Enterprise Windows Servers (EWS) - is an infrastructure information system and provides a hosting a platform for major applications that supports USPTO systems.

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

TPS-IS includes four applications used to support USPTO staff through the trademark review process. TPS-IS features the ability to interface with related systems within USPTO. The information systems are:

First Action System for Trademarks 2 (FAST2): FAST2 serves the USPTO Trademark Legal Instruments Examiner (LIE), their Supervisors (SLIE), and the Intent to Use (ITU) staff. LIEs are personnel that perform reviews and update trademark cases. Each LIE is

assigned to a law office where a system is needed to aid them in processing the work item associated with trademark cases. The FAST2 system allows LIEs to process the work items assigned to them. FAST2 presents the LIEs with a list of work items and allows them to choose items to process. When processing a work item, the FAST2 system allows the user to view and/or edit case information in related systems. It processes the PII data collected by TPS-ES as part of the trademark application process.

Trademark Cropped Image Management (TCIM): TCIM accepts cropped images from Trademark Electronic Application System (TEAS), the Trademark Data Entry and Update System (TRADEUPS), and the Data Management Branch of the Office of System Network Management. The images are stored in a directory structure based on the serial number of the associated trademark application. The TCIM database keeps an inventory of the stored image files and the date each file was received. It does not process PII data.

Trademark Image Capture and Retrieval System (TICRS): TICRS is designed to capture, store, retrieve, and print digital images of trademark application documents. TICRS has the following logical components: (1) the capture component enables the input of digital images by scanning paper and the capture of index data; (2) the storage component manages the physical storage of images and provides access control to maintain security; and (3) the retrieval component provides query and output capabilities for applications within the system. The information in the system is exported to a PDF document and given to the USPTO Webmaster to post onto the USPTO public website. Through USPTO's website, the public is able to query the PDF document to determine active fastener insignias. It processes the PII data collected by TPS-ES as part of the trademark application process.

Trademark Data Entry and Update System (TRADEUPS): TRADEUPS is used for new application data entry and the editing of bibliographic data and Trademark text. The system is designed to interface with the TRM database and the USPS address verification software to verify that the correspondence address submitted by an applicant is deliverable. TRADEUPS includes those data elements and functions required to process new applications in the re-Examination Section. It processes the PII data collected by TPS-ES as part of the trademark application process.

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

TPS-IS uses client/server and web-based interfaces to access the information in the system.

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

TPS-IS information systems use Hypertext Transfer Protocol (HTTP) and Transmission Control Protocol/Internet Protocol (TCP/IP) for transmitting to and from the system over the USPTO internal network. All data in transit is encrypted and all requests that are made are automatically re-directed to HTTP Secure (HTTPS).

(g) Any information sharing

TPS-IS shares trademark application data with USPTO's Trademark Processing System – External Systems (TPS-ES) and Trademark Next Generation (TMNG) and the public via the TRM database. The bureau shares the PII in the IT system within the bureau via direct access and give the public access to the non-sensitive PII in the system on a case-by-case basis.

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

35 U.S.C. § 2; 15 U.S. C. § Chapter 22; 37 CFR § 2.

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

The FIPS 199 security categorization for TPS-IS is 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. Gender	☐	k. Telephone Number	☒	r. Criminal Record	☐
e. Age	☐	l. Email Address	☒	s. Marital Status	☐
f. Race/Ethnicity	☐	m. Education	☐	t. Mother's Maiden Name	☐
g. Citizenship	☒	n. Religion	☐		
u. Other general personal data (specify):					

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

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	☐	f. Scars, Marks, Tattoos	☐	k. Signatures	☐

b. Palm Prints	☐	g. Hair Color	☐	l. Vascular Scans	☐
c. Voice/Audio Recording	☐	h. Eye Color	☐	m. DNA Sample or Profile	☐
d. Video Recording	☐	i. Height	☐	n. Retina/Iris Scans	☐
e. Photographs	☐	j. Weight	☐	o. Dental Profile	☐
p. Other distinguishing features/biometrics (specify):					

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

Other Information (specify)

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

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

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

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

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

Information is provided directly by the individuals about whom the information pertains and they certify the accuracy of the information upon submission. The system 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, and auditing). Mandatory 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 screening. 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. Inactive accounts will be deactivated and roles will be deleted from the application.

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. 0651-0009: Applications for Trademark Registration 0651-0027: Recording Assignments 0651-0028: Fastener Quality Act Insignia Record Process 0651-0048: Native American Tribal Insignia 0651-0050: Response to Office Action and Voluntary Amendment Forms 0651-0051: Madrid Protocol 0651-0054: Substantive Submissions Made During the Prosecution of the Trademark Application 0651-0055: Post Registration 0651-0056: Submissions Regarding Correspondence and Regarding Attorney Representation 0651-0061: Trademarks Petitions
☐	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).

Applicant information stored in the system are about members of the public. USPTO employees and contractors working in the system also have their names in the system.

Addresses and e-mail addresses are used for correspondence and as authorization for the Office to send correspondence concerning the application to the applicant or applicant's attorney. The system collects trademark application data such as the applicant's name and address, and legal entity such as a corporation, partnership, LLC, etc.

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 attach against the system by adversarial or foreign entities, any potential PII data stored within the system could be exposed. To avoid a breach, the system has certain security controls in place to ensure the information is handled, retained, and disposed of appropriately. Access to individual's PII is controlled through the application, and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. 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 and any suspicious indicators such as browsing will be immediately investigated and appropriate action taken. Also, system users undergo annual mandatory training regarding appropriate handling of information.

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

	security awareness procedure training for all employees. All offices 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: This PIA serves as notice. A notice is also provided by a warning banner when the employee or contractor logs into the workstation before accessing the TPS-IS system. This notice is provided to internal USPTO employees and contractors only. See banner in APPENDIX A.
☐	No, notice is not provided.	Specify why not:

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

☐	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
☒	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: Individuals grant consent by filling out a trademark registration and submitting it for processing. They are notified that some of the information that they submit will become public information. They may decline to provide PII by not submitting a trademark registration for processing.

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: Consent is given at the front-end systems.

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

☐	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how:
☒	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: Consent is given at the front-end systems.

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): 5/23/2024 ☐ 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 4 Appendix J recommended

	security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
☒	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
☒	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
☒	Contracts with customers establish DOC ownership rights over data including PII/BII.
☒	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
☐	Other (specify):

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

PII within the system is secured using appropriate management, operational, and technical safeguards in accordance with NIST requirements. Such management controls include a 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/BII 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 authorized 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/USPTO-26, Trademark Application and Registration Records
☐	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: • N1-241-06-2:2: Trademark Case File Records and Related Indexes, selected • N1-241-06-2:3: Trademark Case File Records and Related Indexes, non-selected • N1-241-06-2:4: Trademark Case File Feeder Records and Related Indexes • N1-241-06-2:5: Trademarks Routine Subject Files • N1-241-05-2:5: Information Dissemination Product Reference • GRS 5.1, item 020: Non-Recordkeeping Copies of Electronic Records • GRS 5.2, item 020: Intermediary 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: The combination of name, home address, citizenship, email address, job title, etc., can easily identify a particular person.
☒	Quantity of PII	Provide explanation: The quantity of PII contained in this system is large enough to require adequate protection.
☒	Data Field Sensitivity	Provide explanation: The PII data fields when combined would have an adverse effect on the organization or individuals if a loss were to occur.
☒	Context of Use	Provide explanation: The personally identifiable information processed by TPS-IS is used to identify the individuals or companies that have registered trademarks with the government of the United States.
☒	Obligation to Protect Confidentiality	Provide explanation: Based on the data fields and in accordance with the Privacy Act of 1974, PII must be protected. The sensitive PII in the system needs certain security and privacy controls. Sensitive information found in the system is protected through access control and Disk Level encryption.
☒	Access to and Location of PII	Provide explanation: Government employees and contractors have direct access to the PII. Access is limited only to the identified and authenticated users and partners.
☐	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data,

include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

The PII in this system poses a risk if exposed. System users undergo annual mandatory training regarding appropriate handling of information. Physical access to servers is restricted to only a few authorized individuals. The 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.

Appendix A: Warning Banner