Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
Trademark External

Reviewed by: Jamie Holcombe

☒ 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: 2025.02.25 11:32:41 -05'00' 2/25/2025

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO Trademark External

Unique Project Identifier: TPL-TE-02-00

Introduction: System Description

Provide a brief description of the information system.

TM External Search is comprised of different search components, described below:

TM External Filing (eFile): is an electronic application filing system for United States Patent and Trademark Office (USPTO) Trademarks. It provides the USPTO customers to electronically complete and submit a variety of trademark forms using a web-based user interface. eFile allows the customer to first select then fill out a specific Trademark form, check the form for completeness, and submit the form directly to the USPTO via the Internet to make an official filing online. eFile is the replacement system for the legacy Trademark intake system (TEAS/TEASi). Please note that USPTO is in the process of changing the name of eFile to Trademark Center.

Trademark Last Updated Service (TM-LUS): is a service that allows customers, Application Programming Interface (API) users, to retrieve information about a given trademark application when it was last updated. Currently the service returns the latest prosecution history, and case status update dates. Users can request two types of response formats, JavaScript Object Notation or Extensible Markup Language. Users can also submit multiple serial numbers up to 25 max. TM-LUS disseminates public information and does not implement authorization or authentication.

TM-LUS is built on the USPTO Amazon Web Service (AWS) Cloud Services (UACS) platform and utilizes AWS services through UACS. It exposes REST based services that users can query for publicly available Trademark information using Hypertext Transfer Protocol Secure (HTTP) Uniform Resource Locator (URL). Since the nature of the data exposed by this service is public by default, the application does not require any authorization and authentication from the end users. TM-LUS gets its data from TSDR On-Prem services over HTTPS protocol.

The TM Pre-Examinations Application (TM-PEA): component is a cloud solution with a User Interface (UI) component available to internal LIE examiners only. It will reduce the unprecedented backlog of trademark applications awaiting Pre-Examination by leveraging robotic process automation (RPA), Natural Language Process (NLP), and Machine learning (ML) to automate the pseudo mark process. It filters out trademark applications that do not require a pseudo mark because the applied mark consists entirely of American English words by routing these applications directly to examination. TM-PEA aims to reduce by 20-30% of the approximate daily incoming 4K applications per day, and expedite processing for future

applications that do not require a pseudo mark. Pseudo mark recommendations are generated and displayed in TRADEUPS for Pre-Examiners to leverage.

Trademark Electronic Official Gazette (TM-EOG): component is a cloud solution with multiple modules that helps servicing publication domain data. The Publication-processor: application is a batch process application that is run on a schedule. The purpose of the batch processes is to move Official Gazette (OG) records through a publication workflow resulting in those cases being published in the TM-EOG application. The Publication-sync-svcs: application is a batch process executed nightly to cache a fresh copy of the state and country validation data from the ITC API. This is to support validation activities performed by the publication-processor. The Publication-management applications manages ETL batch operations for daily processing of publication data workflow. It uses steps functions in AWS as means of tracing process completion and error handling as well as addressing try mechanisms.

TM-Notification Services (TM-NS): TM Notification Services (TM-NS) is a backend enterprise business & data service provider. It provides subscribing clients with services to send email to pre-determined sender addresses, it is leveraged on Form Paragraph Template TM-NS process to construct communication and coordinate letter correspondence with USTPO mail office, updates prosecution history with communication sent, upload artifact sample of email or letter in Content Management System (CMS) to display artifact in TSDR as case content documents. In addition, this component host functionality for the creation of TM-Snapshot which registers a view of the data/image at a point in time when particular transactions are executed. These snapshots are stored in Content Management System (CMS) for applicant viewing.

Trademark Design Search Code Manual (TM-DSCM): is an Internet-accessible database. It is a Web-based application that allows public access to search and retrieve design search codes.

Address the following elements:

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

Trademark External is a master system that includes a collection of search applications that provide different search capabilities.

(b) System location

USPTO AWS Cloud Services (UACS) in the East/West region (US region).

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

Trademark External is interconnected to:

All sub-system's interconnections

Fee Processing Next Generation (FPNG): to process fee payments for eFile filings.

ID.me: this system provides external authentication and authorization services to TM-External applications.

Identity, Credential, and Access Management (ICAM): The mission of ICAM is to provide an enterprise authentication and authorization services to all applications.

USPTO Amazon Cloud Services (UACS): The UACS Infrastructure-as-a-Service (IaaS) platform used to support USPTO Information Systems hosted in the Amazon Web Services (AWS) East/West environment. UACS leverages AWS 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. The AWS East/West environment is comprised of several sub-components including, Virtual Private Cloud (VPC), Elastic Cloud Computing (EC2), Identity and Authentication Management (IAM), and Simple Storage Service.

TM-CMS Services: for submission of eFile binary attachment files associated with a filing. TM-CMS is a centralized document management system for Trademarks.

Trademark Next Generation (TMNG): TMNG is an application information system that provides support for the automated processing of trademark applications for the USPTO. TMNG provides users with bibliographic data in a standard markup form, business reporting and dashboard data sources. Publishing features are available to enable consumer's access to published data in the official gazette to review information and search for items of interest. Editing features allow authorized users to perform editing functions (create, modify, delete) that are role-based for searching across current and archival versions. TMNG is also used by Examining Attorneys during the Examination phase of an application TM-COM Services to retrieve trademark data. Trademark Content Management System (CMS) for retrieving trademark documents.

Trademark Processing System (External) Trademark (TPS-ES): eFile connects to a service in Trademark Electronic Application System (TEAS) to retrieve assigned case serial number.

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

Trademark External applications are a collection of interactive search and notification tools that can be classified as web and mobile applications. A typical application consists of a web page supported by all modern web browsers where users key in a certain term related to trademark and that would scan different trademark databases to retrieve relevant information. TM-Mobile is accessed through a mobile with an additional option of getting notification in the mobile device for trademark status updates. How information in the system is retrieved by the user.

EFile provides the USPTO customers a web-based user interface to electronically complete and submit trademark forms. A user is guided through a series of steps in the eFile UI to complete a filing on a trademark case. Filing data is staged in a staging database and then subsequently submitted to other Trademark services through a series of REST API calls.

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

HTTPS within the internal USPTO cloud.

(f) Any information sharing

Data is shared internally to USPTO as listed in the interconnections.

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

Trademark Act, 15 U.S.C. §1051.

(h) 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): The addition of eFile will increase the privacy risk of this system.					

☐ 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): Trademark Case Serial number, last 4 digits of credit card					
*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): mailing address and domicile address					

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): mailing address					

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): e-signature					

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): Any business that applied for a trademark					

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

The accuracy of the information in the system is ensured by obtaining the information directly from the source individual applicants. Access controls, including the concept of least privilege, are in place within the system to protect the integrity of this data as it is processed or stored. The responsibility falls under the front facing customer interacting applications where the information is verified during the authentication and ID proofing process. 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 0651-0050 Response to Office Action 0651-0056 Trademark Submissions Regarding Correspondence and Regarding Attorney Representation 0651-0086 Trademark Modernization Act
☐	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 no 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): For internal system consumption and for correspondence with the interested party. User PII data is associated with trademark case filling in order to identify the interested parties.			

Section 5: Use of the Information

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

The bibliographic information stored in the system about applicants for a trademark is used to uniquely identify the registrant's trademark. Addresses and e-mail addresses are used for correspondence and an authorization for the Office to send correspondence concerning the application to the applicant or applicant's attorney. As anyone may register a trademark, the information may reference a federal employee, contractor, member of the public or a foreign national.

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. 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. An audit trail is generated when the database is accessed. These audit trails are based on the applications server out-of-the-box logging reports reviewed by the Information System Security Officer (ISSO) and System Auditor 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.

☒	TM-External connects with and receives data from TPS-ES, TMNG, and TM-CMS. The information transmitted between the systems is protected within USPTO's secure perimeter through the USPTO AWS Cloud Services, Network and Security Infrastructure (NSI) and the Security and Compliance Services (SCS). FPNG ICAM ID.Me
☐	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): Individual with whom the information pertains.			

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: Privacy Policy and notice is provided through the OKTA Log-in see appendix 1
☐	No, notice is not provided.	Specify why not: Customer Interfacing applications are responsible for individual interactions to review/update PII/BII

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 are not able to decline to provide PII/BII, as the information collected is necessary for the processing of trademark applications.

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: Individuals are not able to consent to particular uses of their PII/BII as all PII/BII collected is necessary for the processing of trademark applications.

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: Individuals have the opportunity to review/update PII/BII pertaining to them for eFile, prior to the applications submission, through logging into their account and updating the information, this is only possible prior to the submission of the application.
☒	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: Individuals do not have the opportunity to review/update PII/BII pertaining directly in eFile, after submission. Once the application is submitted the individuals would need to amend

		the information via TEAS. For the other sub-systems individuals do not have the opportunity to update the information directly in the system but can update through the customer Interfacing applications.

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): 3/29/2024 ☐ 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).*

The USPTO uses the Life Cycle review process to ensure that management controls and are in place for Trademark Systems including Trademark Content Management Center components. During the enhancement of any component, the security controls are reviewed, re-evaluated, and updated in the Security Plan. The Security Plan specifically addresses the controls that are in place, and planned, during the operation of the enhanced system. Additional management controls include performing national agency checks on all personnel, including contractor staff. A Security Categorization compliant with the FIPS 199 and NIST SP 800-60 requirements was conducted for Trademark systems. The overall FIPS 199 security impact level for Trademark systems was determined to be Moderate. This categorization influences the level of effort needed to protect the information managed and transmitted by the system.

Operational controls include securing all hardware associated with the Trademark systems in the USPTO Data Center. The Data Center is controlled by access card entry and is manned by a uniformed guard service to restrict access to the servers, their operating systems, and databases. Backups are managed by the Enterprise Tape Backup System (ETBS) and are secured off-site by First Federal. Windows and Linux servers within Trademark systems are regularly updated with the latest security patches by the Windows and Unix System Support Groups.

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-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.)*

☒	There is an approved record control schedule. N1-241-06-2:4: Trademark Case File Feeder Records and Related Indexes GRS 4.1.010: Tracking and Control 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: Employee ID, Name, Telephone Number, Email Number, Occupation and Job Title can be used to identify an individual.
☒	Quantity of PII	Provide explanation: PII is collected as part of trademark submission for association and correspondence purposes. With each trademark application, the USPTO receives multiple data points. The USPTO receives hundreds of thousands of applications each year with at least 600,000 applications annually since 2018.
☒	Data Field Sensitivity	Provide explanation: The personally identifiable information Stored in TRM database is public record information.
☒	Context of Use	Provide explanation:

		The personally identifiable information Stored in TRM database 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: In accordance with the Privacy Act of 1974, USPTO Privacy Policy requires the PII information collected within the system to be protected in accordance with NIST SP 800-122 and NIST SP 800-53 Rev5, Guide to Protecting the Confidentiality of Personally Identifiable Information.
☒	Access to and Location of PII	Provide explanation: Access to PII stored in eFile and TRM databases are only accessible to internal individuals and applications with proper access level.
☐	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 low 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.

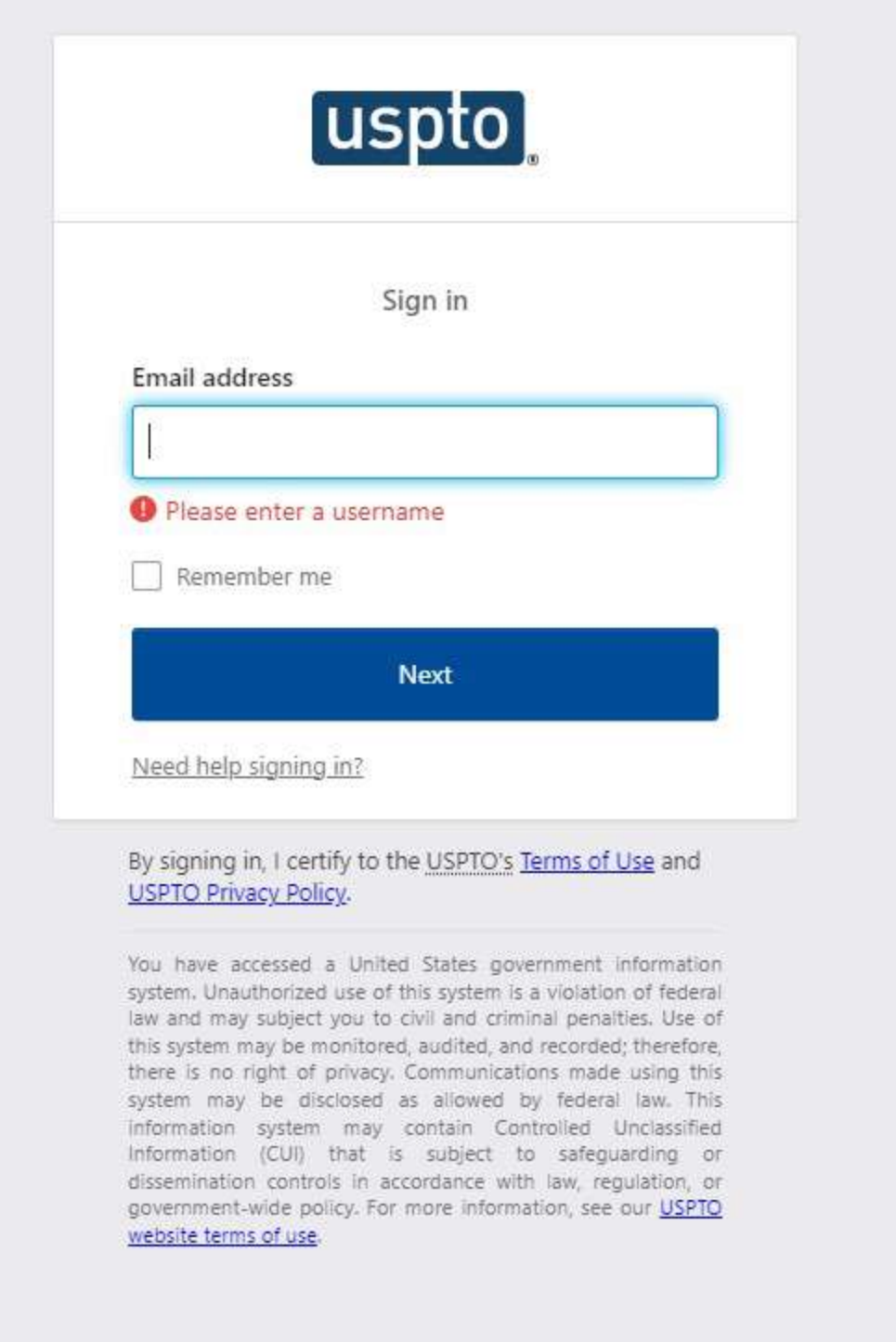
12.2 Indicate whether the conduct of this PIA results in any required business process changes.

☐	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 1


uspto
Sign in
Email address
Please enter a username
Remember me
Next
Need help signing in?
By signing in, I certify to the USPTO's Terms of Use and USPTO Privacy Policy.
You have accessed a United States government information system. Unauthorized use of this system is a violation of federal law and may subject you to civil and criminal penalties. Use of this system may be monitored, audited, and recorded; therefore, there is no right of privacy. Communications made using this system may be disclosed as allowed by federal law. This information system may contain Controlled Unclassified Information (CUI) that is subject to safeguarding or dissemination controls in accordance with law, regulation, or government-wide policy. For more information, see our USPTO website terms of use.