Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
Trademark Exam (TM-EXM)

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: 2023.12.26 11:43:46 -05'00' 10/23/2023

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO Trademark Exam (TM-EXM)

Unique Project Identifier: (TPL-TMEXM-01-00)

Introduction: System Description

Provide a brief description of the information system.

Trademark Exam (TM-EXM) is a center where trademark attorneys and professional staff have the ability to securely login and complete end-to-end review and processing of trademark applications/registrations. Trademark Exam provides the ability to manage workload, conduct searches of multiple databases, update/change application/registration data, communicate with internal business units and with applicants/registrants, check and update application/registration statuses, and process fees and refunds. TM-EXM consists of the following components:

TM-EXM-TRS – Provides backend API services to enable other Trademark systems to replace their use of TRAM. Trademark applicants PII derives from TM-COM.
TM-EXM-Ruby – Provides a role-based access to editing data for Trademark applications and registrations in a web application user interface. All the PII/BII originate from TM-COM. If there are mistakes, TM-EXM Ruby allows USPTO employee/contractor to manually amend PII/BII within TM-COM via TRS.
TM-EXM-Search-UI –Enable examiners to review trademarks. Examiners will not be able to view trademark applications. (No PII)
TM-EXM-TMSBE – Trademark Search Backend is the backend service for Search-UI, which will not contain PII/BII.
TM-EXM-TESS-UI (planned) – Public version of Search-UI that does not include PII.
TM-EXM-TDSCM (planned) – Trademark design search code manual provides the instructions and procedures for coding and interpreting the design search code. TM-EXM-TDSCM is a static web application that is available to both internal and external users.
TM-EXM-Onyx (planned) – Onyx runs queries determined by attorneys for special marks, and deliver query results to the attorneys. The user interface allows for the attorneys to manage special mark queries.
TM-EXM-Pearl (planned) – Provides a role-based access to editing data for petitions in a web application user interface.

Examiners, which includes DOC employees and contractors, will have direct access to members of the public's PII and BII who have submitted a Trademark application. Examiners will use PII and BII from section 2.1 to process Trademark applications from members of the public.

Address the following elements:

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

(b) System location

USPTO AWS Cloud Services (UACS) US East/West

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

Interconnects with other systems, which includes the following.

PTO-TPL-TC-Trademark Common Services (TM-COM): TM-COM provides APIs for other USPTO systems to access trademark application. TM-EXM-TRS uses this information to replace functionality in the TRAM system that is being retired.

PTO-TPL-Trademark Next Generation-Content Management System (TMNG-CMS): TMNG-CMS provides a content repository for all TMNG internal systems. Relational DB access to Trademark and Exam process data. TM-EXM will be reading and updating as examiners process a trademark application. TRM database is the database for the Trademark product line and stores the process flow for all Trademark products, including TM-EXM.

PTO-EIPL-DS-ICAM-IDaaS ICAM Identity as a Service (OKTA): The ICAM IDaaS is an Infrastructure information system, and provides authentication and authorization. TM-EXM will be using it for authenticating users.

PTO-EIPL-IHSC-UACS-USPTO AWS Cloud Services (UACS): UACS provides an AWS environment that is preconfigured on top of AWS to meet many of the security controls for ATO. This allows developers to more quickly develop microservices that provide value to the agency as they then only need to focus on the controls specific to their microservice. TM-EXM will being UACS to build and host the applications.

Interconnections that use TM-EXM microservices:

PTO-TPL-TMNG Trademark Next Generation (TMNG): TMNG is an application information system that provides support for the automated processing of trademark applications for the USPTO. It will be using TM-EXM-TRS for processing of trademark applications. It will be using TM-EXM-TDSCM for conducting trademark searches.

TMeOG-Trademark Electronic Official Gazette (subsystem): Official Gazette supports notification to the public about pending trademark applications. It uses TM-EXM-TRS for processing of trademark applications.

PTO-EBPL-IPLMSS-TTABIS Trademark Trial and Appeal Board Information System(subsystem): TTABIS is a system that provides integrated information support by

processing proceedings for the Trademark Trial and Appeal Board (TTAB). This includes generating actions and tracking the status of proceedings, as well as recording data and issuing reports. It uses TM-EXM-TRS for TTAB proceedings.

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

Trademark Exam accomplish its mission through the use of web applications and microservices in a cloud environment (Amazon Web Services). TM-EXM-Onyx connects to TM-EXM-TMSBE. Particular Trademark Exam components (TM-EXM-TRS, TM-EXM-Pearl, and TM-EXM-TDSCM) provide backend shared services that will integrate with existing USPTO applications. Trademark attorneys will use TM-EXM-Ruby web application to accomplish their mission. The public will use TM-EXM-TESS-UI to search public trademark information.

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

Other systems/applications will utilize API calls to retrieve information from TM-EXM-TRS, TM-EXM-Onyx, TM-EXM-Pearl, TM-EXM-TMSBE, and TM-EXM-TDSCM. Users retrieve information from TM-EXM-Pearl, TM-EXM-Ruby, TM-EXM-Search-UI, and TM-EXM-TESS-UI via a web user interface.

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

Information is transmitted to and from the system via HTTPS/TLS.

(g) Any information sharing

The only sharing is by other USPTO applications that are not publicly available.

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

Trademark Act, 15 U.S.C. §§1051-1054, 1061-1063, 1091-1096, 1126

(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. 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.

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.
☒	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).

Trademark Exam (TM-EXM) is a center where trademark attorneys and professional staff have the ability to securely login and complete end-to-end review and processing of trademark applications/registrations. Trademark Exam provides the ability to manage workload, conduct searches of multiple databases, update/change application/registration data, communicate with

internal business units and with applicants/registrants, check and update application/registration statuses, and process fees and refunds. TM-EXM consists of the following components:

TM-EXM-TRS – Provides backend API services to enable other Trademark systems to replace their use of TRAM. Trademark applicants PII derives from TM-COM.
TM-EXM-Ruby – Provides a role-based access to editing data for Trademark applications and registrations in a web application user interface. All the PII/BII originate from TM-COM. If there are mistakes, TM-EXM Ruby allows USPTO employee/contractor to manually amend PII/BII within TM-COM via TRS.
TM-EXM-Search-UI –Enable examiners to review trademarks. Examiners will not be able to view trademark applications. (No PII)
TM-EXM-TMSBE – Trademark Search Backend is the backend service for Search-UI, which will not contain PII/BII.
TM-EXM-TESS-UI (planned) – Public version of Search-UI that does not include PII.
TM-EXM-TDSCM (planned) – Trademark design search code manual provides the instructions and procedures for coding and interpreting the design search code. TM-EXM-TDSCM is a static web application that is available to both internal and external users.
TM-EXM-Onyx (planned) – Onyx runs queries determined by attorneys for special marks, and deliver query results to the attorneys. The user interface allows for the attorneys to manage special mark queries.
TM-EXM-Pearl (planned) – Provides a role-based access to editing data for petitions in a web application user interface.

Examiners, which includes DOC employees and contractors, will have direct access to members of the public's PII and BII who have submitted a Trademark application. Examiners will use PII and BII from section 2.1 to process Trademark applications from members of the public.

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. These audit events are sent to USPTO organizational-wide SIEM and monitoring is performed by USPTO's Compliance team. 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, encryption is used to secure the during transmission. 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: The system connects to the following USPTO systems: PTO-TPL-TC-Trademark Common Services (TPL-TC-01-00) PTO-EIPL-DS-ICAM-IDaaS ICAM Identity as a Service (EIPL-DS-03-00) PTO-TPL-TMNG Trademark Next Generation (PTOT-004-00)->PTO-TPL-Trademarks Next Generation - Examination (PTOT-004-08) PTO-TPL-TMNG Trademark Next Generation (PTOT-004-00)->PTO-TPL-TMNG-TMeOG-Trademark Electronic Official Gazette (PTOT-004-02) PTO-EBPL-IPLMSS-TTABIS Trademark Trial and Appeal Board Information System (PTOL-001-10) NIST security controls are in place to ensure that information is handled, retained, and disposed of appropriately. For example, encryption is used to secure the during transmission. 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: Notice is provided to the individuals through the source system, eFile, where their PII/BII was originally collected.
☐	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: An individual's right to decline to provide PII/BII is determined by the source system, eFile. The individuals do not have the right to restrict eFile from sharing the PII/BII with TM-EXM. TM-EXM requires the PII/BII to fulfil the purpose for which the individual submitted the information.

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: The individual's rights to consent to particular uses of their PII/BII is determined by the source system. The individuals do not have the right to restrict source system from sharing the PII/BII with TM-EXM. TM-EXM requires the PII/BII to fulfil the purpose for which the individual submitted the 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:
☒	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: Individuals rights to review/update PII/BII are determined by the source system. Though individuals may review the PII/BII pertaining to them within TM-EXM, if the individual requires an update to their PII/BII they would need to resolve that with the source system.

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: tracked in system 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): ☒ 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 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)*: PAT-TM-17, USPTO Security Access Control and Certificate Systems. PAT-TM-18, USPTO Personal Identification Verification (PIV) and Security Access Control Systems 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. 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: Trademarks Routine Subject Files
☐	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): other methods as the hardware team sees fit			

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: millions of records
☒	Data Field Sensitivity	Provide explanation: The personally identifiable information Displayed by TM-EXM is public record information.
☒	Context of Use	Provide explanation: TM-EXM-Search-UI: Allows users to search for existing marks TM-EXM-TRS: TRS is required to provide services to other internal trademark applications so that they can replace use of TRAM TM-EXM-Ruby: Ruby is required to allow editing of trademark data that currently is not possible in other Trademark applications TM-EXM-TESS-UI (planned): allows public users to search for existing marks TM-EXM-Onyx (planned): Onyx is required to provide Trademarks a way of identifying special characters TM-EXM-Pearl (planned): Pearl is required to provide Trademarks a way of handling petition TM-EXM-TDSCM (planned): allows users to search Design Search Codes Manual and retrieve the search results
☒	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: AWS Cloud

☐	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.