Template Version Number: 01-2021

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

Privacy Threshold Analysis
for the
Madrid Cloud

U.S. Department of Commerce Privacy Threshold Analysis

USPTO Madrid Cloud

Unique Project Identifier: TPL-TI-01-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system: *Provide a brief description of the information system.*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

The TM Exam International Center supports the exchange of data and the requirements specific to the Madrid protocol. Madrid Cloud provides processing for electronic communications between the International Bureau (IB) and USPTO Trademark Attorneys concerning U.S. based Applications for International Registration and extensions of International Registrations into the United States.

The Madrid Protocol is an international trademark filing and registration agreement designed to simplify and reduce the costs of foreign trademark filing. The Madrid Protocol secures protection for the international registration of marks and is organized by the International Bureau (IB), a division of the World Intellectual Property Organization (WIPO).

Address the following elements:

a) *Whether it is a general support system, major application, or other type of system*
   Madrid Cloud is a major application.

b) *System location*
   Madrid Cloud is located in USPTO AWS Cloud (UACS).

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

   Madrid Cloud interconnects with the systems listed below:

   - **Trademark Processing System – Internal System (TPS-IS)** is an information system that provides support for the automated processing of trademark applications for the USPTO. TPS-IS includes applications that are used to support USPTO staff through the trademark review process. TPS-IS features the ability to interface with related systems within USPTO.

- **Intellectual Property Leadership Management Support System (IPLMSS)** is a Major Application that facilitates grouping and management of 10 separate information system boundaries that collectively support the USPTO Director, Deputy Director, Office of the General Counsel (OGC), including OGC's components the Office of General Law (OGL), Office of the Solicitor, and Office of Enrollment and Discipline (OED), Trademark Trial and Appeal Board (TTAB), Patent Trial and Appeal Board (P-TACTS); Office of Patent Training (OPT); and Office of Policy and International Affairs (OPIA).
- **Trademark Processing System – External Systems (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.

d) The purpose that the system is designed to serve

The system is designed to facilitate the USPTO's agreement under the Madrid Protocol with the International Bureau (IB) and all undersigned countries. The TM International system provides a gateway for U.S.-based applicants seeking trademark protection in one or more of the countries in the Agreement, and also for any foreign-based applicants in one of the undersigned countries to seek trademark protection within the United States.

e) The way the system operates to achieve the purpose

Trademark (TM) International operates by sending applications to and receiving applications from the IB. The applications are routed based on transaction type. The transactions sent from USPTO to the IB are called "outbound" transactions; whereas, the transactions sent to USPTO from the IB are called "inbound" transactions. Some transactions are automatically certified, and others may require a manual review. When a manual review is required, staff in the Madrid Processing Unit (MPU) leverage the user interface, Madrid Certification Review Program (MCRP), to manually certify an application.

f) A general description of the type of information collected, maintained, used, or disseminated by the system

The system collects, maintains, uses, and disseminates information about a trademark application and applicant needed to file internationally or receive from the international board and file within the U.S, e.g. Name, Email, Address, Phone.

g) Identify individuals who have access to information on the system

PTO employees and contractors have access to the system.

h) How information in the system is retrieved by the user

The Madrid Cloud uses web services to transmit information. The workflow engine can be viewed in a web browser console for status of various process instances by administrative users and operations and maintenance team.

i) How information is transmitted to and from the system

Madrid Cloud transmits information to and from other systems through legacy socket layer protocols, Secure File Transfer Protocol (sftp), and via emails to applicants and representatives. Applicants are automatically notified of the status of their applications.

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

☒ This is a new information system. *Continue to answer questions and complete certification.*

☐ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

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. *Continue to answer questions and complete certification.*

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

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

☒ Yes. This is a new information system.

☐ Yes. This is an existing information system for which an amended contract is needed.

☐ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

☐ No. This is not a new information system.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

☐ Yes. *(Check all that apply.)*

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

☒ No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?
As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

☒ Yes, the IT system collects, maintains, or disseminates BII.

☐ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?
As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

☒ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

☒ DOC employees
☒ Contractors working on behalf of DOC
☐ Other Federal Government personnel
☒ Members of the public

☐ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

☐ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
Provide the legal authority which permits the collection of SSNs, including truncated form.

☒ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

☒ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

☐ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

☐ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

☒ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

☒ The criteria implied by one or more of the questions above **apply** to the Madrid Cloud and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

☐ The criteria implied by the questions above **do not apply** to the Madrid Cloud and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

System Owner Name: Donald Ulrich Office: Office of Application Engineering and Development Phone: (571) 272-1093 Email: Donald.Ulrich@uspto.gov Signature: Users, Ulrich, Donald Digitally signed by Users, Ulrich, Donald Date: 2022.04.14 10:00:07 -04'00' Date signed: _____	**Chief Information Security Officer** Name: Don Watson Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-8130 Email: Don.Watson@uspto.gov Signature: Users, Watson, Don Digitally signed by Users, Watson, Don Date: 2022.04.18 20:14:20 -04'00' Date signed: _____
Privacy Act Officer Name: Ezequiel Berdichevsky Office: Office of General Law (O/GL) Phone: (571) 270-1557 Email: Ezequiel.Berdichevsky@uspto.gov Signature: Users, Berdichevsky, Ezequiel Digitally signed by Users, Berdichevsky, Ezequiel Date: 2022.04.05 11:23:17 -04'00' Date signed: _____	**Bureau Chief Privacy Officer and Co-Authorizing Official** Name: Henry J. Holcombe Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-9400 Email: Jamie.Holcombe@uspto.gov Signature: Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry Date: 2022.04.19 09:08:58 -04'00' Date signed: _____
Co-Authorizing Official Name: David S. Gooder Office: Office of the Commissioner for Trademarks Phone: (571) 270-0980 Email: David.Gooder@uspto.gov Signature: Users, Gooder, David S. Digitally signed by Users, Gooder, David S. Date: 2022.04.27 15:27:13 -04'00' Date signed: _____	