

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



**Privacy Impact Assessment
for the
Madrid Cloud**

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

Jennifer Goode 7/13/2022

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

U.S. Department of Commerce Privacy Impact Assessment USPTO Madrid Cloud

Unique Project Identifier: TPL-TI-01-00

Introduction: System Description

Provide a brief description of the information system.

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

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.

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

The Madrid Cloud microservices exclusively use representation state transfer (REST) for retrieval downstream, e.g. the MCRP client application. The workflow engine can be viewed in a web browser console for status of various process instances by administrative users and Operations and Maintenance (O&M).

(f) 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.

(g) Any information sharing

Trademark (TM) International operates by sending applications to and receiving applications from the IB via a secure channel. 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, PTO employees in the Madrid Processing Unit (MPU) leverage the user interface, Madrid Certification Review Program (MCRP), to manually certify an application.

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

The Trademark Act of 1946, Madrid Protocol Implementation Act of 2002, and E-Government Act provide specific programmatic authorities.

(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	<input type="checkbox"/>	d. Significant Merging	<input type="checkbox"/>	g. New Interagency Uses	<input type="checkbox"/>
b. Anonymous to Non-Anonymous	<input type="checkbox"/>	e. New Public Access	<input type="checkbox"/>	h. Internal Flow or Collection	<input type="checkbox"/>
c. Significant System Management Changes	<input type="checkbox"/>	f. Commercial Sources	<input type="checkbox"/>	i. Alteration in Character of Data	<input type="checkbox"/>
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*	<input type="checkbox"/>	f. Driver's License	<input type="checkbox"/>	j. Financial Account	<input type="checkbox"/>
b. Taxpayer ID	<input type="checkbox"/>	g. Passport	<input type="checkbox"/>	k. Financial Transaction	<input type="checkbox"/>
c. Employer ID	<input type="checkbox"/>	h. Alien Registration	<input type="checkbox"/>	l. Vehicle Identifier	<input type="checkbox"/>
d. Employee ID	<input type="checkbox"/>	i. Credit Card	<input type="checkbox"/>	m. Medical Record	<input type="checkbox"/>
e. File/Case ID	<input checked="" type="checkbox"/>				
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	<input checked="" type="checkbox"/>	h. Date of Birth	<input type="checkbox"/>	o. Financial Information	<input type="checkbox"/>
b. Maiden Name	<input type="checkbox"/>	i. Place of Birth	<input type="checkbox"/>	p. Medical Information	<input type="checkbox"/>
c. Alias	<input type="checkbox"/>	j. Home Address	<input checked="" type="checkbox"/>	q. Military Service	<input type="checkbox"/>
d. Gender	<input type="checkbox"/>	k. Telephone Number	<input checked="" type="checkbox"/>	r. Criminal Record	<input type="checkbox"/>
e. Age	<input type="checkbox"/>	l. Email Address	<input checked="" type="checkbox"/>	s. Marital Status	<input type="checkbox"/>
f. Race/Ethnicity	<input type="checkbox"/>	m. Education	<input type="checkbox"/>	t. Mother's Maiden Name	<input type="checkbox"/>
g. Citizenship	<input checked="" type="checkbox"/>	n. Religion	<input type="checkbox"/>		
u. Other general personal data (specify):					

--

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

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

System Administration/Audit Data (SAAD)					
a. User ID	<input checked="" type="checkbox"/>	c. Date/Time of Access	<input checked="" type="checkbox"/>	e. ID Files Accessed	<input type="checkbox"/>
b. IP Address	<input checked="" type="checkbox"/>	f. Queries Run	<input checked="" type="checkbox"/>	f. Contents of Files	<input type="checkbox"/>
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	<input type="checkbox"/>	Hard Copy: Mail/Fax	<input type="checkbox"/>	Online	<input type="checkbox"/>
Telephone	<input type="checkbox"/>	Email	<input type="checkbox"/>		
Other (specify):					

Government Sources					
Within the Bureau	<input checked="" type="checkbox"/>	Other DOC Bureaus	<input type="checkbox"/>	Other Federal Agencies	<input type="checkbox"/>
State, Local, Tribal	<input type="checkbox"/>	Foreign	<input checked="" type="checkbox"/>		
Other (specify):					

Non-government Sources			
Public Organizations	<input type="checkbox"/>	Private Sector	<input type="checkbox"/>
Commercial Data Brokers	<input type="checkbox"/>		
Third Party Website or Application	<input type="checkbox"/>		
Other (specify):			

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

Madrid Cloud 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 screen. The USPTO maintains an audit trail and performs random, periodic reviews (quarterly) to identify unauthorized access and changes as part of verifying the integrity of administrative account holder data and roles. Inactive accounts will be deactivated and roles will be deleted from the application.

2.4 Is the information covered by the Paperwork Reduction Act?

<input checked="" type="checkbox"/>	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. The original collection of the data (via TPS-ES) is covered by 0651-0051, Madrid Protocol
<input type="checkbox"/>	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	<input type="checkbox"/>	Biometrics	<input type="checkbox"/>
Caller-ID	<input type="checkbox"/>	Personal Identity Verification (PIV) Cards	<input type="checkbox"/>
Other (specify):			

<input checked="" type="checkbox"/>	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	<input type="checkbox"/>	Building entry readers	<input type="checkbox"/>
Video surveillance	<input type="checkbox"/>	Electronic purchase transactions	<input type="checkbox"/>

Other(specify):

There are not any IT systems 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	<input type="checkbox"/>	For administering human resources programs	<input type="checkbox"/>
For administrative matters	<input checked="" type="checkbox"/>	To promote information sharing initiatives	<input checked="" type="checkbox"/>
For litigation	<input type="checkbox"/>	For criminal law enforcement activities	<input type="checkbox"/>
For civil enforcement activities	<input type="checkbox"/>	For intelligence activities	<input type="checkbox"/>
To improve Federal services online	<input checked="" type="checkbox"/>	For employee or customer satisfaction	<input checked="" type="checkbox"/>
For web measurement and customization technologies (single-session)	<input type="checkbox"/>	For web measurement and customization technologies (multi-session)	<input type="checkbox"/>
Other(specify): It is collected to properly register and receive Trademarks and related intellectual property internationally.			

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).

PTO employees, contractors, and foreign national use Madrid Cloud.

The Madrid Cloud System collects, maintains, or disseminates PII from members of the public who are foreign nationals and also has information about PTO employees and contractors that have access to this systems backend for their routine daily work processes.

PII is used to register and manage trademarks properly to and from the International Board to associate holders with intellectual property to improve federal services online and also improve employee/customer satisfaction by easing the administrative process. The information is collected to support administrative matters, to improve Federal services online, to promote information sharing initiatives, and for employee or customer satisfaction.

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 that 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.

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	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DOC bureaus	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Federal agencies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
State, local, tribal gov't agencies	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Private sector	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign governments	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign entities	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other (specify): International Board	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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?

<input type="checkbox"/>	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
<input checked="" type="checkbox"/>	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
<input type="checkbox"/>	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.

<input checked="" type="checkbox"/>	<p>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:</p> <p>TPS-ES, IPLMSS, and TPS-IS are authorized to process PII. Technical controls are provided in the relevant IT System Security and Privacy Plan (SSPP)/Dynamic Operational Support Plans (DOSP).</p> <p>Madrid Cloud has put security controls 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. The following are current USPTO policies; Information Security Foreign Travel Policy (OCIO-POL-6), IT Privacy Policy (OCIO- POL-18), IT Security Education Awareness Training Policy (OCIO-POL-19), Personally Identifiable Data Removal Policy (OCIO-POL-23), USPTO Rules of the Road (OCIO-POL- 36). 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.</p>
<input type="checkbox"/>	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	<input type="checkbox"/>	Government Employees	<input checked="" type="checkbox"/>
Contractors	<input checked="" type="checkbox"/>		
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.)*

<input checked="" type="checkbox"/>	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
<input checked="" type="checkbox"/>	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 .	
<input type="checkbox"/>	Yes, notice is provided by other means.	Specify how:
<input type="checkbox"/>	No, notice is not provided.	Specify why not:

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

<input checked="" type="checkbox"/>	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Individuals grant consent by filing out a trademark registration and submitting it for processing. They are notified that the information that they submit will become public information. They may decline to provide PII by not submitting a trademark registration for processing.
<input type="checkbox"/>	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

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

<input checked="" type="checkbox"/>	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: All information collected is for contact purpose. Individuals have a choice of what contact information to give. They are also made aware that the information provided will be made public.
<input type="checkbox"/>	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

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

<input checked="" type="checkbox"/>	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Individuals are informed they may contact USPTO to update their records for contact information changes.
<input type="checkbox"/>	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

<input type="checkbox"/>	All users signed a confidentiality agreement or non-disclosure agreement.
<input checked="" type="checkbox"/>	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
<input checked="" type="checkbox"/>	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
<input checked="" type="checkbox"/>	Access to the PII/BII is restricted to authorized personnel only.
<input checked="" type="checkbox"/>	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Audit logs

<input checked="" type="checkbox"/>	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): _____ <input checked="" type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
<input checked="" type="checkbox"/>	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
<input checked="" type="checkbox"/>	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).
<input checked="" type="checkbox"/>	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
<input checked="" type="checkbox"/>	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
<input type="checkbox"/>	Contracts with customers establish DOC ownership rights over data including PII/BII.
<input type="checkbox"/>	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
<input type="checkbox"/>	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 the life cycle 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 authorize personnel. The system maintains an audit trail and the appropriate personnel is alerted when there is suspicious activity. Data is encrypted in transit and at rest.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

- Yes, the PII/BII is searchable by a personal identifier.
- No, the PII/BII is not searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, “the term ‘system of records’ means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.”

<input checked="" type="checkbox"/>	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. <i>(list all that apply):</i> PAT-TM-26, Trademark Application and Registration Records
<input type="checkbox"/>	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
<input type="checkbox"/>	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.)*

<input checked="" type="checkbox"/>	There is an approved record controls schedule. Provide the name of the record controls schedule: <ul style="list-style-type: none"> • N1-241-06-2:4, Trademark Case File Feeder Records and Related Indexes • GRS 5.2, item 010: Transitory records
<input type="checkbox"/>	No, there is not an approved record controls schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
<input checked="" type="checkbox"/>	Yes, retention is monitored for compliance to the schedule.
<input type="checkbox"/>	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	<input type="checkbox"/>	Overwriting	<input type="checkbox"/>
Degaussing	<input type="checkbox"/>	Deleting	<input checked="" type="checkbox"/>
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.)*

<input checked="" type="checkbox"/>	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
<input type="checkbox"/>	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

<input type="checkbox"/>	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.)

<input checked="" type="checkbox"/>	Identifiability	Provide explanation: Identifiability is derived from General Personal Data and Work-Related Data, including Name, Home address, Telephone Number, Email Address, Work Address, Work Telephone Number, Work Email Address, Business Associates, and Proprietary or Business Information.
<input checked="" type="checkbox"/>	Quantity of PII	Provide explanation: Thousands of records are received; the PII is publicly available.
<input checked="" type="checkbox"/>	Data Field Sensitivity	Provide explanation: All fields, except for email, are part of the public record. Madrid Cloud doesn't receive or send anything to the IB except the holder's name, address, and email, and the IB Representative information. The only information Madrid Cloud masks is the holder/owner's email address. Madrid Cloud is required to make public the correspondence email address.
<input checked="" type="checkbox"/>	Context of Use	Provide explanation: 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.
<input checked="" type="checkbox"/>	Obligation to Protect Confidentiality	Provide explanation: USPTO Privacy Policy requires the PII information collected within the system to be protected accordance to NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information. In accordance with the Privacy Act of 1974, PII must be protected.
<input checked="" type="checkbox"/>	Access to and Location of PII	Provide explanation: The data is stored in the AWS cloud and is protected by FedRAMP privacy and security controls.
<input type="checkbox"/>	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 threats to the system are insider threats and foreign entities. The information in the system can be retrieved by the public. USPTO implements security and management controls to prevent the inappropriate disclosure of sensitive information. Security controls are employed to ensure information is resistant to tampering, remains confidential as necessary, and is available as intended by the Agency and as expected by authorized users. Management controls are utilized to prevent the inappropriate disclosure of sensitive information. Network and Security Infrastructure (NSI) Security and Compliance Services (SCS) provide additional automated transmission and monitoring mechanisms to ensure that PII/BII information is protected and not breached by external entities.

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

<input type="checkbox"/>	Yes, the conduct of this PIA results in required business process changes. Explanation:
<input checked="" type="checkbox"/>	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.

<input type="checkbox"/>	Yes, the conduct of this PIA results in required technology changes. Explanation:
<input checked="" type="checkbox"/>	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

<p>System Owner Name: Donald Ulrich Office: Office of Application Engineering and Development Phone: (571) 272-1093 Email: Donald.Ulrich@uspto.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: <u>Users, Ulrich, Donald</u> <small>Digitally signed by Users, Ulrich, Donald Date: 2022.04.14 09:59:28 -04'00'</small></p> <p>Date signed: _____</p>	<p>Chief Information Security Officer Name: Don Watson Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-8130 Email: Don.Watson@uspto.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: <u>Users, Watson, Don</u> <small>Digitally signed by Users, Watson, Don Date: 2022.04.18 20:15:13 -04'00'</small></p> <p>Date signed: _____</p>
<p>Privacy Act Officer Name: Ezequiel Berdichevsky Office: Office of General Law (O/GL) Phone: (571) 270-1557 Email: Ezequiel.Berdichevsky@uspto.gov</p> <p>I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA.</p> <p>Signature: <u>Users, Berdichevsky, Ezequiel</u> <small>Digitally signed by Users, Berdichevsky, Ezequiel Date: 2022.04.05 11:26:07 -04'00'</small></p> <p>Date signed: _____</p>	<p>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</p> <p>I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.</p> <p>Signature: <u>Users, Holcombe, Henry</u> <small>Digitally signed by Users, Holcombe, Henry Date: 2022.04.19 09:07:42 -04'00'</small></p> <p>Date signed: _____</p>
<p>Co-Authorizing Official Name: David S. Gooder Office: Office of the Commissioner for Trademarks Phone: (571) 270-0980 Email: David.Gooder@uspto.gov</p> <p>I certify that this PIA accurately reflects the representations made to me herein by the System Owner, the Chief Information Security Officer, and the Chief Privacy Officer regarding security controls in place to protect PII/BII in this PIA.</p> <p>Signature: <u>Users, Gooder, David S.</u> <small>Digitally signed by Users, Gooder, David S. Date: 2022.04.26 14:16:51 -04'00'</small></p> <p>Date signed: _____</p>	

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.