Template Version Number: 01-2021

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

## Privacy Impact Assessment
## for the
## Trademark Processing System – External Systems (TPS-ES)

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

Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry
Date: 2022.03.14 13:18:37 -04'00'

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

# U.S. Department of Commerce Privacy Impact Assessment
# USPTO Trademark Processing System – External Systems (TPS-ES)

**Unique Project Identifier: PTOT-002-00**

## Introduction: System Description

*Provide a brief description of the information system.*

TPS-ES is a Major Application that provides customer support for processing Trademark applications for USPTO. TPS-ES includes six applications that are used to support USPTO staff and public users through the trademark application process. The six applications are described below:

**MADRID Protocol** is an international trademark filing and registration system that was designed to simplify and reduce the costs of foreign trademark filing. This 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).

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

**Trademark Electronic Application System (TEAS)** provides a Web site for electronic filing of Trademark applications. Post submission, TEAS facilitates the transfer of these applications to Trademark Operations for intake processing.

**Trademark Electronic Application System International (TEASi)** is a Web application that provides users the ability to submit trademark applications that are filed under international treaties, satisfying the conditions and requirements of the MADRID Protocol Implementation Act and of the Office of Trademarks.

**Trademark Electronic Search System (TESS)** provides public access to search for pending and abandoned Trademark applications and registration.

**Trademark Identification Manual (TIDM)** provides trademark examiners and the general public with a web-based interface for searching the Trademark Identification Manual.

Address the following elements:

***(a) Whether it is a general support system, major application, or other type of system***
TPS-ES is a Major Application.

***(b) System location***
The components of TPS-ES are primarily located at 600 Dulany Street, Alexandria, Virginia.

***(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)***
The TPS-ES is a Major Application information system, and provides customer support for processing Trademark applications for USPTO.

**Security and Compliance Services (SCS):** SCS provides Security Incident and Event Management, Enterprise Forensic, Enterprise Management System, Security and Defense, Enterprise Scanner, Enterprise Cybersecurity Monitoring Operations, Performance Monitoring Tools, Dynamic Operational Support Plan, & Situational Awareness and Incident Response.

**Enterprise Windows Services (EWS)**: EWS is an Infrastructure information system which provides a hosting platform for major applications that support various USPTO missions.

**Network and Security Infrastructure System (NSI)**: NSI is an Infrastructure information system and provides an aggregate of subsystems that facilitates the communications, secure access, protective services, and network infrastructure support for all United States Patent and Trademark Office (USPTO) IT applications.

**Database Services (DBS):** DBS is an Infrastructure information system and provides a Database Infrastructure to support mission of USPTO database needs.

**Enterprise Software Services (ESS)**: ESS is a major application which provides an architecture capable of supporting current software services at USPTO.

**Information Dissemination Support System (IDSS)**: IDSS is a major application system which provides automated support for the timely search and retrieval of electronic text and images concerning patent applications and patents by USPTO internal and external users.

**Intellectual Property Leadership Management System (IPLMSS)**: IPLMSS is a major application which groups and manages seven separate subsystems to provide tools to cull and organize large amounts of legal data, to support FOIA, Privacy Act requests and appeals, to docket and track cases, manage library content, route electronic notices, develop and maintain assessments, and to register and maintain the practitioner roster and monitor practitioner disciplinary action.

**Service Oriented Infrastructure (SOI)**: SOI is a general support system and infrastructure information system that provides the underlying services for a mobile, feature-rich, and stable platform upon which USPTO applications can be deployed.

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

**Trademark Processing System – Internal System (TPS IS):** TPS-IS is an application information system and provides support for the automated processing of trademark applications for the USPTO.

**World Intellectual Property Organization (WIPO):** The World Intellectual Property Organization or WIPO is a UN specialized agency created in 1967 to promote intellectual property (IP) protection and encourage creative activity all over the world. WIPO is basically a global forum for IP policy, services, information and cooperation.

**Trilateral Network (TRINET):** TRINET disseminates unpublished patent application information and priority documents in regards to the application process. TRINET is an Infrastructure information system, and provides secure network connectivity for electronic exchange and dissemination of patent data between authenticated endpoints at the Trilateral Offices and TRINET members. The Trilateral Offices consist of the United States Patent and Trademark Office (USPTO), the European Patent Office (EPO), and the Japanese Patent Office (JPO). The TRINET members consist of the World Intellectual Property Office (WIPO), the Canadian Intellectual Property Office (CIPO) and the Korean Intellectual Property Office (KIPO). All members sign an MOU agreement to share patent information through end user access and credentials provided by USPTO TRINET.

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

The system operates to achieve the purpose through the below systems.

**Trademark Madrid System (MADRID)** - MADRID assists the Office of Trademark in sending and receiving data from International Bureau (IB)-related to international applications that are being handled by the U.S. Patent and Trademark Office (USPTO).

**Trademark Design and Search Code Manual (TDSCM)** - TDSCM is a web-based application that allows trademark examining attorneys and the general public to search and retrieve design search codes from the TDSCM's Design Search Codes Manual.

**Trademark Electronic Application System (TEAS) and Trademark Electronic Application System International (TEASi) -** TEAS and TEASi provide customers with the means to electronically complete and register a trademark domestically or internationally. The applicant's information is stored and is publically available for trademark discovery via TDSCM and Trademark Electronic Search System. Bibliographic information collected from trademark registrants, include:

- The applicant's name and address.
- The applicant's legal entity.

The following information can be collected from trademark registrants but is not required in order to submit the trademark for processing:

- If the applicant is a partnership, the names and citizenship of the applicant's general partners.
- The entity's address for correspondence.
- An e-mail address for correspondence and an authorization for the Office to send correspondence concerning the application to the applicant or applicant's attorney by e-mail (only business email addresses are published).

The information is collected to uniquely identify the registrant of a trademark. The information becomes part of the official record of the application and is used to document registrant location and for official communications. After the application has been filed, the information is part of the public record and a member of the public may request a copy of the application file. However, applicants are informed and sign a consent that the information given will be accessible to the public. *Please see "Appendix A" for warning banner statement.*

**Trademark Electronic Search System (TESS)** - TESS is designed to provide the public with the capability to search text and images of pending, registered, and dead Trademark applications via internet browser.

**Trademark Identification Manual (TIDM)** - The Trademark Identification Manual (TIDM) system is a component that provides trademark examiners and the public with a web-based interface for searching and retrieving the text of the Trademark Classification Manual.

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

TPS-ES uses web-based interfaces to access the information in the system. Some subsystems also provide web APIs to retrieve information in an automated fashion.

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

TPS-ES uses HTTPS for transmitting to and from the system over the USPTO internal network, as well as the public internet.

***(g) Any information sharing***

TPS-ES shares trademark application data with Trademark Processing System – Internal Systems (TPS-IS), where the primary data repository resides.

TPS-ES shares international trademark data with IB, both sending and receiving internationally registered trademarks.

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

35 U.S.C. § 2; 15 U.S. C. § 1051 et seq.; 37 CFR § 2.21.

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

The FIPS 199 security categorization for TPS-ES is Moderate.

## Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

☐ This is a new information system.

☐ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

| Changes That Create New Privacy Risks (CTCNPR) | | | | | |
|---|---|---|---|---|---|
| a. Conversions | ☐ | d. Significant Merging | ☐ | g. New Interagency Uses | ☐ |
| b. Anonymous to Non-Anonymous | ☐ | e. New Public Access | ☐ | h. Internal Flow or Collection | ☐ |
| c. Significant System Management Changes | ☐ | f. Commercial Sources | ☐ | i. Alteration in Character of Data | ☐ |
| j. Other changes that create new privacy risks (specify): | | | | | |

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

☒ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment.

## Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

| Identifying Numbers (IN) | | | | | |
|---|---|---|---|---|---|
| a. Social Security* | ☐ | f. Driver's License | ☐ | j. Financial Account | ☐ |
| b. Taxpayer ID | ☐ | g. Passport | ☐ | k. Financial Transaction | ☐ |
| c. Employer ID | ☐ | h. Alien Registration | ☐ | l. Vehicle Identifier | ☐ |
| d. Employee ID | ☐ | i. Credit Card | ☐ | m. Medical Record | ☐ |
| e. File/Case ID | ☐ | | | | |
| n. Other identifying numbers (specify): | | | | | |

| |
|---|
| *Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form: |

| **General Personal Data (GPD)** | | | | | |
|---|---|---|---|---|---|
| a. Name | ☒ | h. Date of Birth | ☐ | o. Financial Information | ☐ |
| b. Maiden Name | ☐ | i. Place of Birth | ☐ | p. Medical Information | ☐ |
| c. Alias | ☐ | j. Home Address | ☒ | q. Military Service | ☐ |
| d. Gender | ☐ | k. Telephone Number | ☒ | r. Criminal Record | ☐ |
| e. Age | ☐ | l. Email Address | ☒ | s. Marital Status | ☐ |
| f. Race/Ethnicity | ☐ | m. Education | ☐ | t. Mother's Maiden Name | ☐ |
| g. Citizenship | ☒ | n. Religion | ☐ | | |
| u. Other general personal data (specify): | | | | | |

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

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

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

| **Other Information (specify)** |
|---|
| |
| |

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

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

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

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

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

| |
|---|
| The information is provided directly by the individuals about whom the information pertains and they certify the accuracy of the information upon submission. 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. |

2.4 Is the information covered by the Paperwork Reduction Act?

| | |
|---|---|
| ☒ | Yes, the information is covered by the Paperwork Reduction Act.<br>Provide the OMB control number and the agency number for the collection.<br>0651-0009 Applications for Trademark Registration<br>0651-0050 Response to Office Action & Voluntary Amendment Forms<br>0651-0051; Madrid Protocol<br>0651-0054: Substantive Submissions Made During the Prosecution of the Trademark Application<br>0651-0055: Post Registration<br>0651-0056: Submissions Regarding Correspondence and Regarding Attorney Representation<br>0651-0061: Trademarks Petitions |
| ☐ | No, the information is not covered by the Paperwork Reduction Act. |

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

| Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD) | | | |
|---|---|---|---|
| Smart Cards | ☐ | Biometrics | ☐ |
| Caller-ID | ☐ | Personal Identity Verification (PIV) Cards | ☐ |
| Other (specify): | | | |

| | |
|---|---|
| ☒ | There are not any technologies used that contain PII/BII in ways that have not been previously deployed. |

## Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

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

| | |
|---|---|
| ☒ | 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).

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 as a means 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.)

The information is published to the public and submitters of information are made aware of this beforehand. Foreign entities, adversarial entities and insider threats are the threats to privacy within this system. Inadvertent private information exposure is a risk and USPTO has policies, procedures, and training to ensure that employees are aware of their responsibility of protecting sensitive information and the negative impact to the agency if there is a loss, misuse, or unauthorized access to or modification of sensitive private information. USPTO requires Annual Security Awareness Training for all employees as well as policies and procedures documented in the Cybersecurity Baseline Policy. All USPTO offices adhere to 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.<br>Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:<br><br>TRINET, WIPO, IPLMSS, TPS-IS, TMNG, IDSS, ESS, SCS<br><br>During processing, the information is passed through to various internal information systems (see Introduction, question (c)) for processing at the USPTO. The information is not routinely shared with other agencies before publication, though the registrants can check on the progress of their applications.<br><br>The servers storing the potential PII are located in a highly sensitive zone within the USPTO internal network and logical access is segregated with network firewalls and switches through an Access Control list that limits access to only a few approved authorized accounts. USPTO monitors in real-time all activities and events within the servers storing the potential PII data and a subset of USPTO Cyber security personnel review audit logs received on a regular bases and alert the information System Security Officer (ISSO) and/or the appropriate personnel when inappropriate or unusual activity is identified. Access is restricted on a "need to know" basis. Active Directory security groups are utilized to segregate users in accordance with their job functions. |
| ☐ | 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: A notice is provided by a warning banner when the applicant accesses the application to submit a Trademark registration. In addition, a consent form is signed by the applicant giving USPTO the authority to share the information provided with the public. *Please see "Appendix A" for details on warning banner.* |
| ☐ | 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: 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.<br>They may decline to provide PII by not submitting a trademark registration for processing. |
| ☐ | 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.

| | | |
|---|---|---|
| ☒ | 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. |
| ☐ | 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.

| | | |
|---|---|---|
| ☒ | Yes, individuals have an opportunity to | Specify how: Individuals will need to work with USPTO if |

| | | |
|---|---|---|
| | review/update PII/BII pertaining to them. | contact information changes to update their records. |
| ☐ | 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.)*

| | |
|---|---|
| ☐ | 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.<br>Explanation: Audit Logs |
| ☒ | The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements.<br>Provide date of most recent Assessment and Authorization (A&A): ___March 30, 2021_____<br>☐ This is a new system. The A&A date will be provided when the A&A package is approved. |
| ☒ | The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher. |
| ☒ | NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M). |
| ☒ | A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks. |
| ☒ | Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy. |
| ☐ | Contracts with customers establish DOC ownership rights over data including PII/BII. |
| ☒ | Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers. |
| ☐ | Other (specify): |

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

The USPTO uses the Life Cycle review process to ensure that management controls are in place for TPS-ES. 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 management, operational and technical 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 Federal Information Processing Standards (FIPS) 199 and National Institute of Standards and Technology (NIST) SP 800-60 requirements was conducted for TPS-ES. The overall FIPS 199 security impact level for TPS-ES 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 TPS-ES 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. Application servers within TPS-ES are regularly updated with the latest security patches by the Operational Support Groups. Additional operational controls include performing national agency checks on all personnel, including contractor staff.

## 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).<br>Provide the SORN name, number, and link. *(list all that apply)*:<br><br>COMMERCE/PAT-TM-23: User Access for Web Portals and Information Requests<br><br>COMMERCE/PAT-TM-26/USPTO-26: Trademark Application and Registration Records |
| ☐ | Yes, a SORN has been submitted to the Department for approval on (date). |
| ☐ | No, this system is not a system of records and a SORN is not applicable. |

## Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

| | |
|---|---|
| ☒ | There is an approved record control schedule.<br>Provide the name of the record control schedule:<br>N1-241-06-2:2: Trademark Case File Feeder Records and Related Indexes, selected<br>N1-241-06-2:3: Trademark Case File Feeder Records and Related Indexes, non-selected<br>N1-241-06-2:4: Trademark Case File Feeder Records and Related Indexes<br>N1-241-06-2:5: Trademark Routine Subject Files<br>N1-241-05-2:5: Information Dissemination Product Reference |

| | |
|---|---|
| ☐ | No, there is not an approved record control schedule.<br>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:<br>Name, Home address, Telephone number, email address, work address, work email address, and work phone number together can identify a particular individual. |
| ☒ | Quantity of PII | Provide explanation:<br>The PII is publicly available and varies depends on amount of applications. |
| ☒ | Data Field Sensitivity | Provide explanation:<br>The data includes limited personal and work related elements and does not include sensitive identifiable information since all the information processed by TPS-ES is public record information. |
| ☒ | Context of Use | Provide explanation:<br>The personally identifiable information processed by TPS-ES 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:<br>There is no obligation to protect the confidentiality of the personally identifiable information; the PII processed by TPS-ES is public record information. |
| ☒ | Access to and Location of PII | Provide explanation:<br>The PII on this system is available to the general public through the patent website. |
| ☐ | 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 sensitive PII in the system are insider threats and foreign entities. The non-sensitive 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. NSI and 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.

| | |
|---|---|
| ☐ | Yes, the conduct of this PIA results in required business process changes.<br>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.<br>Explanation: |
| ☒ | No, the conduct of this PIA does not result in any required technology changes. |

# Points of Contact and Signatures

**System Owner**
Name: Donald Ulrich
Office: Trademark Systems Division
Phone: 571- 272-1093
Email: Donald.Ulrich@uspto.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: Users, Ulrich, Donald Digitally signed by Users, Ulrich, Donald Date: 2022.03.09 09:36:01 -05'00'

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

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: Users, Watson, Don Digitally signed by Users, Watson, Don Date: 2022.03.13 12:31:10 -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

I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA.

Signature: Users, Berdichevsky, Ezequiel Digitally signed by Users, Berdichevsky, Ezequiel Date: 2022.03.07 11:07:22 -05'00'

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

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.

Signature: Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry Date: 2022.03.14 13:18:57 -04'00'

Date signed: _____

**Co-Authorizing Official**
Name: David S. Gooder
Office: Trademark Systems Division
Phone: (571) 270-0980
Email: David.Gooder@uspto.gov

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.

Signature: Users, Gooder, David S. Digitally signed by Users, Gooder, David S. Date: 2022.03.14 17:58:55 -04'00'

Date signed: _____

**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.**