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

## Privacy Impact Assessment
## for the
## Information Dissemination Support System
## PTOD-001-00

Reviewed by: John B. Owens II, Senior Agency Official for Privacy

☐ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

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

# U.S. Department of Commerce Privacy Impact Assessment
# USPTO Information Dissemination Support System

**Unique Project Identifier: PTOD-001-00**

## **<u>Introduction</u>: System Description**

*Provide a description of the system that addresses the following elements:*
*The response must be written in plain language and be as comprehensive as necessary to describe the system.*
*[Guidance: When completing this section, be sure to include only information suitable for public viewing since this is to be posted online. Do not include system information such as IP addresses, architecture diagrams, et.]*

*(a) a general description of the information in the system*

Information Dissemination Support System (IDSS) is a Major Application (MA) that supports the Trademark and Electronic Government Business Division, the Corporate Systems Division (CSD), the Patent Search System Division, the Office of Electronic Information Products, and the Office of Public Information Services. IDSS 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. IDSS handles current and historical data for patent and trademark applications, whether assigned, certified, issued, or not. It contains interfaces to share data with other information systems throughout the PTOnet and the Internet. IDSS is considered a business-essential system with a Federal Information Processing Standard (FIPS) 199 security categorization of Moderate.

IDSS implements a large, distributed and complex computing environment and each of its automated information systems (AIS) physically reside on a collection of hardware and software components, and services, with various interfaces. The system uses the USPTO's network infrastructure to allow interaction between its subordinate information systems.

*(b) a description of a typical transaction conducted on the system*
Information Dissemination

*(c) any information sharing conducted by the system*
None

*(d) a citation of the legal authority to collect PII and/or BII*
N/A

*(e) the Federal Information Processing Standard (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): N/A no new privacy risks introduced. | | | | | |

## 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* | ☐ | e. File/Case ID | ☐ | i. Credit Card | ☒ |
| b. Taxpayer ID | ☐ | f. Driver’s License | ☐ | j. Financial Account | ☐ |
| c. Employer ID | ☐ | g. Passport | ☐ | k. Financial Transaction | ☒ |
| d. Employee ID | ☐ | h. Alien Registration | ☐ | l. Vehicle Identifier | ☐ |
| m. Other identifying numbers (specify): | | | | | |
| *Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:<br>N/A – IDSS does not collect, store or process Social Security Numbers (SSNs). | | | | | |
| *If SSNs are collected, stored, or processed by the system, please explain if there is a way to avoid such collection in the future and how this could be accomplished: N/A | | | | | |

| **General Personal Data (GPD)** | | | | | |
|---|---|---|---|---|---|
| a. Name | ☒ | g. Date of Birth | ☐ | m. Religion | ☐ |
| b. Maiden Name | ☐ | h. Place of Birth | ☐ | n. Financial Information | ☒ |
| c. Alias | ☐ | i. Home Address | ☒ | o. Medical Information | ☐ |
| d. Gender | ☐ | j. Telephone Number | ☒ | p. Military Service | ☐ |
| e. Age | ☐ | k. Email Address | ☒ | q. Physical Characteristics | ☐ |
| f. Race/Ethnicity | ☐ | l. Education | ☐ | r. Mother’s Maiden Name | ☐ |
| s. Other general personal data (specify): | | | | | |

| **Work-Related Data (WRD)** N/A | | | | | |
|---|---|---|---|---|---|
| a. Occupation | □ | d. Telephone Number | □ | g. Salary | □ |
| b. Job Title | □ | e. Email Address | □ | h. Work History | □ |
| c. Work Address | □ | f. Business Associates | □ | | |
| i. Other work-related data (specify): | | | | | |

| **Distinguishing Features/Biometrics (DFB)** N/A | | | | | |
|---|---|---|---|---|---|
| a. Fingerprints | □ | d. Photographs | □ | g. DNA Profiles | □ |
| b. Palm Prints | □ | e. Scars, Marks, Tattoos | □ | h. Retina/Iris Scans | □ |
| c. Voice Recording/Signatures | □ | f. Vascular Scan | □ | i. Dental Profile | □ |
| j. 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 | □ | d. Queries Run | □ | f. Contents of Files | □ |
| g. Other system administration/audit data (specify): | | | | | |

| **Other Information (specify)** |
|---|
| Type of Assignment transaction (sale, lien, merger, and many others) |
| |
| |

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 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** | | | |
|---|---|---|---|
| To determine eligibility | ☒ | 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).

Information collected is used to process transactions, manage customer orders, document delivery, retrieve data, and capture documents related to the ownership of intellectual properties for both patents and trademarks. The intended use is to carry out the duties of the USPTO as outlined in 35 U.S.C. concerning the dissemination of information, and more specifically, to provide for public customer call center services. This includes tracking responses to customer requests. Data is used to ensure quality customer service for general agency information and assistance. This includes quality control purposes. In addition, the information may be used to conduct surveys of customer experience and satisfaction, and to obtain customer service recommendations.

## 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 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: |
| ☒ | No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII. |

6.3 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: ______________________________________________. | |
| ☐ | Yes, notice is provided by other means. | Specify how: |
| ☒ | No, notice is not provided. | Specify why not: PII is entered by users. |

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: Information is provided on a voluntary basis. While providing this information is voluntary, if the requested information is provided in whole or part, USPTO may not be able to complete the identity or registration process, or complete it in a timely manner. |
| ☐ | 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 requested is provided on a voluntary basis. |
| ☐ | 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 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: Information is used by users only. |

## <u>Section 8</u>: 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: Suspicious system log behavior and log failures are reported to the appropriate personnel to troubleshoot and remediate the issue. |
| ☒ | The information is secured in accordance with FISMA requirements.<br>Provide date of most recent Assessment and Authorization (A&A): <u>June 2015</u><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 (POAM). |
| ☒ | Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy. |
| ☐ | Contracts with customers establish 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.

The information is in accordance with the NIST 800-53, Revision 4 control set. Security Assessment and Authorization activities are routinely conducted for IDSS. Secured technical architecture is incorporated into the system to prevent any unauthorized access to pending cases. Data is maintained in areas accessible only to authorize personnel and systems are password protected.

Management Controls:

1. The USPTO uses the Life Cycle review process to ensure that management controls are in place for IDSS. During the enhancement of any component, the security controls are reviewed, re-evaluated, and updated in the Security Plan. The Security Plans specifically address 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 check on all personnel, including contractor staff.

2. The USPTO Personally Identifiable Data Extracts Policy

Operational Controls:

1. Automated operational controls include securing all hardware associated with IDSS 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. Contingency planning has been prepared for the data. Backups are performed on the processing databases. Backups are stored on tape and are secured off-site. Additional operation controls include: (1) Logical edit checks to ensure proper sequence of actions; (2) Physical terminal identification; (3) Database UserID; (4) Restricted data display, as required; and (5) Restricted access.
2. Manual procedures shall be followed for handling extracted data containing sensitive PII which is physically transported outside of the USPTO premises. In order to remove data extracts containing sensitive PII from USPTO premises, users must:
    a. Maintain a centralized office log for extracted datasets that contain sensitive PII. This log must include the date the data was extracted and removed from the facilities, a description of the data extracted, the purpose of the extract, the expected date of disposal or return, and the actual date of return or deletion.
    b. Ensure that any extract which is no longer needed is returned to USPTO premises or securely erased, and that this activity is recorded on the log.
    c. Obtain management concurrence in the log, if an extract aged over 90 days is still required.
    d. Store all PII data extracts maintained on an USPTO laptop in the encrypted My Documents directory. This includes any sensitive PII data extracts downloaded via the USPTO Virtual Private network (VPN).
    e. Encrypt and password-protect all sensitive PII data extracts maintained on a portable storage device (such as CD, memory key, flash drive, etc.).

Exceptions due to technical limitations must have the approval of the Office Director and alternative protective measures must be in place prior to removal from USPTO premises.

USPTO has not developed a centralized logging system for PII data extracts. Such a system would track the following categories of information:

a. Who performed the extract,
b. When extract was done,
c. What was the extract,
d. Where was the extract taken from,
e. Has the extract been deleted and,
f. If not deleted after 90 days, to monitor that it is still needed in 90 day intervals.

Until a system is implemented, USPTO is using the following compensating controls to protect PII data:

a. No extracts of sensitive data may be copied on to portable media without a waiver approved by the DoC CIO. The request for a waiver must include specifics as to how the data and device are protected, how long the data will be maintained, and how the data on the device will be deleted when no longer required.
b. All laptop computers allowed to store sensitive data must have full disk encryption.
c. All remote access to public USPTO systems containing sensitive data must be encrypted. All remote access to internal USPTO systems containing sensitive data must fully comply with DoC Remote Access Policy requirements.
d. All flexiplace/telework agreements for working off site require that adequate data protection be in place.

Encrypt and password-protect prior to transmission any sensitive PII data extracts that are sent to an external e-mail address via the Internet. The password key should be forwarded to the recipient in a separate e-mail from the attached file.

## **Section 9**: Privacy Act

9.1 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 and number *(list all that apply)*:<br>COMMERCE/PAT-TM-20 Customer Call Center, Assistance and Satisfaction Survey Records, August 2007. |
| ☐ | Yes, a SORN has been submitted to the Department for approval on <u>(date)</u>. |
| ☐ | No, a SORN is not being created. |

## 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: |
| ☐ | 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: GRC 20 allows agency determination that certain electronic records are authorized for erasure or deletion when they are no longer needed for administrative, legal, audit, or other operational purposes. Electronic records that represent hard copy records can be deleted after expiration of the retention period authorized for the hard copy records. |

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 Levels

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.

| | |
|---|---|
| ☐ | 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 levels. *(Check all that apply.)*

| | | |
|---|---|---|
| ☒ | Identifiability | Provide explanation: |
| ☐ | Quantity of PII | Provide explanation: |
| ☐ | Data Field Sensitivity | Provide explanation: |
| ☐ | Context of Use | Provide explanation: |
| ☐ | Obligation to Protect Confidentiality | Provide explanation: |
| ☐ | Access to and Location of PII | Provide explanation: |
| ☐ | Other: | Provide explanation: |

## **Section 12**: Analysis

12.1 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. |

12.2 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. |