

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



**Privacy Threshold Analysis
for the
Information Dissemination Support System
(IDSS)**

U.S. Department of Commerce Privacy Threshold Analysis

USPTO Information Dissemination Support System

Unique Project Identifier: PTOD-001-00

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

Description of the information system and its purpose: *Provide a general description of the information system in a way that a non-technical person can understand.*

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

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

The Information Dissemination Support System (IDSS) is a Major Application.

b) *System location*

System location is 600 Dulany Street, Alexandria Va. 22314

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

IDSS interconnects with:

- Network Security Infrastructure System (NSI)
- Patent Application Location and Monitoring System (PALM)
- PTO-ESS Enterprise Software Services
- PTO-SIMS Storage Infrastructure Managed Service
- PTO-SOI Service Oriented Infrastructure System
- PTO-TPS-IS - Trademark Processing System (Internal Systems)
- Revenue Accounting and Management System (RAM)
- Trademark Reporting and Monitoring System (TRAM)

d) *The purpose that the system is designed to serve*

The IDSS is an Application information system, and provides the following services or functions in support of the USPTO mission. The purpose of the IDSS system is to support 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. It provides automated support for the timely search and retrieval of electronic text and images concerning patent and trademark applications, patents and trademarks by USPTO internal and external users.

IDSS handles current and historical data for patent and trademark applications, whether assigned, certified, issued, or not. IDSS must protect the data from unauthorized disclosure, alteration, and/or corruption to assure public confidence in USPTO's policies and processes. Additionally, it must also provide information and applications in an efficient, effective, and timely manner. IDSS contains interfaces to share data with other subsystems throughout the PTONet and the Internet.

e) The way the system operates to achieve the purpose

IDSS implements a large, distributed and complex computing environment and that each of its applications resides physically on a collection of hardware and software subsystems, and services, and with various interfaces. IDSS uses the USPTO's network infrastructure to allow interaction between its subordinate subsystems.

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

The type of information collected, maintained, use, or disseminated by the system include public user's name, street address, e-mail address, and telephone number.

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

Individuals who have access to information on the system are USPTO personnel such as patent and trademark examiners, their supporting staff, Public Search Facilities staff users and public users.

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

Users enter orders directly, receive the orders, and make inquiries via the Internet where bulk data can also be downloaded.

i) How information is transmitted to and from the system

Information is transmitted to and from the system via the internet.

Questionnaire:

1. What is the status of this information system?

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

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

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

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

 X This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

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

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

_____ Yes. *Please describe the activities which may raise privacy concerns.*

 X No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

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

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

☒ Companies
☐ Other business entities

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

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

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

☐ DOC employees
☐ Contractors working on behalf of DOC
☐ Members of the public

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

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

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

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

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

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

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

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

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

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

CERTIFICATION

X I certify the criteria implied by one or more of the questions above **apply** to the Information Dissemination Support System (IDSS) and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the Information Dissemination Support System (IDSS) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO): Dawei Jiang

Signature of SO: _____

Date: 5/24/2018

Name of Senior Information Security Officer (SISO): Rami Dillon

Signature of SISO: _____

Date: 5/24/18

Name of Authorizing Official (AO): David Chiles

Signature of AO: _____

Date: 6/7/2018

Name of Bureau Chief Privacy Officer (BCPO): David Chiles

Signature of BCPO: _____

Date: 6/7/2018