

**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 (IDSS)

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 (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

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).

Information Dissemination Support System (IDSS) 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. It 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.

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*

The 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:

Patent Capture and Application Processing System – Examination Support (PCAPS-ES):

A collection of tools that facilitates USPTO examiners’ ability to process, examine and review patent applications.

NSI (Network and Security Infrastructure System): The 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.

SOI (Service Oriented Infrastructure): The SOI provides a feature-rich and stable platform upon which USPTO applications can be deployed.

ESS (Enterprise Software System): Provides Enterprise Directory Services, Role-Based Access Control System, Email as a Service, PTO Exchange Services, Symantec Endpoint Protection, Enterprise SharePoint Services, etc.

PTO-SIMS Storage Infrastructure Managed Service): A Storage Infrastructure information system that provides access to consolidated, block level data storage and files system storage. SIMS is primarily used to enhance storage devices, such as disk arrays, tape libraries, and optical jukeboxes.

PTO-TPS-IS - Trademark Processing System (Internal Systems): The system includes 11 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.

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 each of its applications resides physically on a collection of hardware and software subsystems. 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, used, or disseminated by the system

The type of information collected, maintained, used, or disseminated by the system include public users' names, street addresses, e-mail addresses, and telephone numbers.

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. Status of the Information System

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

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

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions	<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. *Continue to answer questions and complete certification.*
- This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or 01-2017). *Continue to answer questions and complete certification.*

- This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2019 or later). *Skip questions and complete certification.*

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

- Yes. This is a new information system.
- Yes. This is an existing information system for which an amended contract is needed.
- No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.
- No. This is not a new information system.

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

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

- Yes. *(Check all that apply.)*

Activities			
Audio recordings	<input type="checkbox"/>	Building entry readers	<input type="checkbox"/>
Video surveillance	<input type="checkbox"/>	Electronic purchase transactions	<input type="checkbox"/>
Other (specify):			

- No.

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

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

- Yes, the IT system collects, maintains, or disseminates BII.
- No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: “The term PII refers to information that can be used to distinguish or trace an individual’s identity either alone or when combined with other information that is linked or linkable to a specific individual.”

- Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*
 - DOC employees
 - Contractors working on behalf of DOC
 - Other Federal Government personnel
 - Members of the public
- No, this IT system does not collect any PII.

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

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

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

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

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

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

- Yes, the IT system collects, maintains, or disseminates PII other than user ID.
- No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

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

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

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

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

CERTIFICATION

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.

<p>System Owner Name: Diane Park Office: Corporate Systems Implementation Branch (I/AEDCSIB) Phone: (571) 272-5332 Email: Diane.Park@uspto.gov</p> <p>Signature: <u>Diane Park</u> <small>Digitally signed by Diane Park Date: 2021.05.20 13:59:13 -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>Signature: <u>DON R Watson</u> <small>Digitally signed by DON R Watson Date: 2021.05.25 07:45:45 -04'00'</small></p> <p>Date signed: _____</p>
<p>Privacy Act Officer Name: John Heaton Office: Office of General Law (O/GL) Phone: (571) 270-7420 Email: Ricou.Heaton@upsto.gov</p> <p>Signature: <u>Users, Heaton, John (Ricou)</u> <small>Digitally signed by Users, Heaton, John (Ricou) Date: 2021.05.19 20:35:15 -04'00'</small></p> <p>Date signed: _____</p>	<p>Bureau Chief Privacy Officer and 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>Signature: <u>Users, Holcombe, Henry</u> <small>Digitally signed by Users, Holcombe, Henry Date: 2021.05.25 11:29:28 -04'00'</small></p> <p>Date signed: _____</p>
<p>Co-Authorizing Official Name: N/A Office: N/A Phone: N/A Email: N/A</p> <p>Signature: _____</p> <p>Date signed: _____</p>	