

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



**Privacy Threshold Analysis
for the
Data Storage Management System (DSMS)**

U.S. Department of Commerce Privacy Threshold Analysis

USPTO Data Storage Management System (DSMS)

Unique Project Identifier: PTOI-016-00

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).

Data Storage Management System (DSMS) is an infrastructure system that provides archival and storage capabilities securely to the USPTO. The information system is considered an essential component of USPTO’s Business Continuity and Disaster Recovery program. DSMS consists of the following subsystems:

- Boyers Data Capture System (BDCS) – Provides the Production Services Branch (PSB) of the Office of Information Management System (OIMS) the capability to rescan patent documents and to reload an issued patent for display by clients such as the Examiners Automated Search Tool and the Web Enabled Search Tool.
- Enterprise Tape Backup System (ETBS) – Provides a consolidated backup system for the entire USPTO. ETBS provides a mechanism to restore individual servers after a disk ETBS uses VERITAS NetBackup by Symantec to provide a reliable backup system. ETBS utilizes backup servers, tape libraries, and COTS products to back up data generated and stored on USPTO servers.
- Storage Infrastructure System (SIS) – Provides disk-based storage for the USPTO enterprise. It consists primarily of SAN Tier 1, Tier 2, and NAS devices. The SIS also consists of networking infrastructure, which includes SAN Switches and Routers.

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

DSMS is a general support system (GSS)

b) *System location*

United States Patent and Trademark Office, 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)*

DSMS is a backend storage system that consists of three subsystems, BDCS, ETBS, and SIS. DSMS hosts two applications that contain PII, Agency Administrative Support System (AASS) and Enterprise Data Warehouse (EDW). PIAs are available for both of those systems. The other applications hosted by DSMS are: Enterprise Record Management and Data Quality System (ERMDQS); Enterprise Virtual Event Services (EVES); OCIO Program Support System (OCIO-PSS); and Patent Search System – Specialized Search and Retrieval (PSS-SS). None of these systems process or store PII or BII.

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

DSMS is a hosting environment that provides secure archival and storage capabilities to the USPTO.

e) *The way the system operates to achieve the purpose*

DSMS is the hosting environment that BDCS, ETBS, and SIS applications use to provide archive and storage capabilities to USPTO users. DSMS operates in the capacity of tape backup, scanned image and disk-based storage. Information sharing conducted by the system is done only internally to UPSTO; nothing is shared outside.

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

DSMS provides backup for the entire USPTO.

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

DSMS system administrators.

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

The information in the system is retrieved by the user via queries sent by the user.

i) *How information is transmitted to and from the system*

Information is transmitted to and from the system using USPTO Networking infrastructure which includes SAN Switches and Routers.

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.
--

The DSMS system acts as a backup storage application for many systems within USPTO, some of which collect SSN like the HR system.

Provide the legal authority which permits the collection of SSNs, including truncated form.

Executive Order 9397, 35 U.S.C. 1; 5 U.S.C. 301.
--

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 PTA 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 DSMS 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 DSMS and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

<p>System Owner Name: Ian Neil Office: Server & Storage Service Branch (I/SSSB) Phone: (571) 272-5075 Email: Ian.Neil@uspto.gov</p> <p>Signature: <u>Ian Neil</u> <small>Digitally signed by Ian Neil Date: 2021.04.19 11:52:38 -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: 2021.04.19 15:05:28 -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: 2021.04.19 11:10:38 -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: 2021.04.20 07:54:06 -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>	