Template Version Number: 01-2021

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: EIPL-IHSS-01-00

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: *Provide a brief description of the information system.*
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).

The Data Storage Management System (DSMS) is a general support system (GSS), and provides the following services or functions in support of the USPTO mission: Secure environment for archival and storage of data and records vital to USPTOs Business Continuity and Disaster Recovery plan. Each of the (Automated Information System) AISs comprising Data Storage Management provides a different set of capabilities. The DSMS is considered a Business Essential (BE) system. The applications that make up the master system are:

- Enterprise Backup Recovery System (EBRS) - is designed to provide a consolidated backup system for the entire United States Patent and Trademark Office (USPTO). EBRS provides a mechanism to restore individual servers after a disk EBRS uses Cohesity to provide a reliable backup system. EBRS utilizes backup servers, 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 and Tier 2. The SIS also consists of networking infrastructure which includes SAN Switches.

Address the following elements:

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 interconnects to:

Corporate Web Systems (CWS) provides a feature-rich and stable platform that contains the Organizations Websites that are used at USPTO such as Intranet and USPTO external website.

Identity Management Authenticator (ID-AUTH) is an end-to-end system tasked with managing the personal identity credentials of USPTO employees and contractors.

Card Management System (CMS) the personalization and issuance of the smart card identification credentials under Homeland Security Presidential Directive (HSPD - 12).

Enterprise Desktop Platform (EDP) is an infrastructure information system which provides a standard enterprise-wide environment that manages desktops and laptops running on the Windows 7 and Windows 10 operating system (OS), providing United States Government Configuration Baseline (USGCB) compliant workstations.

Database Services (DBS) is an Application information system which provides a Database infrastructure to support the mission of USPTO Database needs. The DBS System is composed of a collection of various versions of Database systems Security and Compliance Services (SCS).

Enterprise Software Services (ESS) system provides an architecture capable supporting current software services as well as provide the necessary architecture to support the growth anticipated over the next five years.

Fee Processing Next Generation (FPNG) will replace the RAM system with 21st Century Technologies and implement flexibility to quickly change business rules and other configuration changes without requiring code changes.

Network Security Infrastructure System (NSI) facilitates the communications, secure access, protective services, and network infrastructure support for all USPTO applications.

Enterprise Unix Servers (EUS) is an infrastructure operating system with a sole purpose of providing a UNIX base hosting platform to support other systems at USPTO.

Enterprise Windows Servers (EWS) is an infrastructure information system which provides a hosting platform for major applications that support various USPTO missions.

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

Patent Search System - Primary Search and Retrieval (PSS-PS) supports legal determination of prior art for patent applications, including text and image search of repositories of US application and grant publications, foreign application and grant publications, various concordances, and non-patent literature. It represents the databases that contain the images and text data for US Patent Grants, published applications, and unpublished applications.

Patent Search System – Specialized Search and Retrieval (PSS-SS) provides access to highly specialized data that may include annual submissions of nucleic and amino acid sequence or prior-art searching of polynucleotide and polypeptide sequences, other types of information that may be more scientific or technology-based, Patent Linguistic Utility Service (a query by example search system), Chemical Drawing ability, and Foreign Patent Data.

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	☐	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.*

☒ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment. *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	☐	Building entry readers	☐
Video surveillance	☐	Electronic purchase transactions	☐
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 and 115; 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

☒ The criteria implied by one or more of the questions above **apply** to the Data Storage Management System (DSMS) and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

☐ The criteria implied by the questions above **do not apply** to the Data Storage Management System (DSMS) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

System Owner Name: Ian Neil Office: Server & Storage Service Branch (I/SSSB) Phone: 571-272-5075 Email: Ian.Neil@uspto.gov Signature: Users, Neil, Ian Digitally signed by Users, Neil, Ian Date: 2023.06.10 00:02:24 -04'00' Date signed: ______________________________	**Chief Information Security Officer** Name: Timothy S. Goodwin Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-0653 Email: Timothy.Goodwin@uspto.gov Signature: Digitally signed by Timothy Goodwin Date: 2023.07.24 08:47:40 -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 Signature: Users, Berdichevsky, Ezequiel Digitally signed by Users, Berdichevsky, Ezequiel Date: 2023.06.27 21:07:39 -04'00' Date signed: ______________________________	**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 Signature: Users, Stephens, Deborah Digitally signed by Users, Stephens, Deborah Date: 2023.07.28 21:18:52 -04'00' Date signed: ______________________________
Co-Authorizing Official Name: N/A Office: N/A Phone: N/A Email: N/A Signature: ______________________________ Date signed: ______________________________	