Template Version Number: 01-2020

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

Privacy Impact Assessment
for the
Data Storage Management System (DSMS)

Reviewed by: Henry J. Holcombe, Bureau Chief Privacy Officer

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

Jennifer Goode 06/09/2021

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO Data Storage Management System (DSMS)

Unique Project Identifier: PTOI-016-00

Introduction: 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.

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, Virginia 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 way the system operates to achieve the purpose(s) identified in Section 4

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 USPTO.

(e) 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.

(f) 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.

(g) Any information sharing conducted by the system

Information sharing conducted by the system is done only internally to UPSTO;

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

The specific programmatic authorities *(statutes or Executive Orders)* for collecting, maintaining, using, and disseminating the information for DSMS is 5 U.S.C. 301, 35 U.S.C. 2, and 44 U.S.C. 3101.

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

FIPS 199 security impact category for DSMS is 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):					

☒ 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.

☐ 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).

☐ 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).

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*	☒	f. Driver's License	☐	j. Financial Account	☒
b. Taxpayer ID	☒	g. Passport	☐	k. Financial Transaction	☒
c. Employer ID	☐	h. Alien Registration	☐	l. Vehicle Identifier	☐
d. Employee ID	☒	i. Credit Card	☒	m. Medical Record	☐
e. File/Case ID	☒				
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form: The data stored in DSMS is based upon the application/system ("front-end system") that uses DSMS for its storage requirements. For those systems that collect SSNs, their need for collection, maintenance, and dissemination is addressed by those front-end systems in their PIAs. DSMS is a back-end storage system that stores the information.					

General Personal Data (GPD)					
a. Name	☒	h. Date of Birth	☒	o. Financial Information	☒
b. Maiden Name	☐	i. Place of Birth	☒	p. Medical Information	☐
c. Alias	☐	j. Home Address	☒	q. Military Service	☐
d. Gender	☐	k. Telephone Number	☒	r. Criminal Record	☐
e. Age	☐	l. Email Address	☒	s. Physical Characteristics	☐
f. Race/Ethnicity	☐	m. Education	☐	t. Mother's Maiden Name	☐
g. Citizenship	☒	n. Religion	☐		
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	☒	e. Work Email Address	☒	i. Business Associates	☒
b. Job Title	☒	f. Salary	☒	j. Proprietary or Business Information	☐
c. Work Address	☒	g. Work History	☒	k. Procurement/contracting records	☐
d. Work Telephone Number	☒	h. Employment Performance Ratings or other Performance Information	☐		
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	☒	f. Scars, Marks, Tattoos	☐	k. Signatures	☐
b. Palm Prints	☐	g. Hair Color	☐	l. Vascular Scans	☐
c. Voice/Audio Recording	☐	h. Eye Color	☐	m. DNA Sample or Profile	☐
d. Video Recording	☐	i. Height	☐	n. Retina/Iris Scans	☐
e. Photographs	☒	j. Weight	☐	o. Dental Profile	☐
p. 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	☐	f. Queries Run	☐	f. Contents of Files	☐
g. Other system administration/audit data (specify): DSMS is the enterprise-wide storage solution for USPTO applications. If snapshots are collected by the system, it is that application's responsibility to receive consent to collect and use.					

Other Information (specify)

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 Describe how the accuracy of the information in the system is ensured.

Personally Identifiable Information in DSMS is secured using appropriate administrative, physical, and technical safeguards in accordance with the applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

All access has role based restrictions, and individuals with access privileges have undergone vetting and suitability screening. Data is maintained in areas accessible only to authorized personnel. The USPTO maintains an audit trail and performs random periodic reviews to identify unauthorized access. Also, integrity verification to detect unauthorized changes is performed as well.

2.4 Is the information covered by the Paperwork Reduction Act?

☐	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
☒	No, the information is not covered by the Paperwork Reduction Act.

2.5 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			
For a Computer Matching Program	☐	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).

DSMS stored data is based upon the application/system that is using DSMS for data storage. The information stored in DSMS is collected and utilized by USPTO application systems. The information can be collected from DOC employees, contractors working on behalf of DOC, other Federal Government personnel, and members of the public. DSMS is a back-end storage system that houses the information.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

DSMS implements security and management controls to prevent the inappropriate disclosure of sensitive information. Automated mechanisms are in place to ensure the security of all stored data. Security controls are employed to ensure information is resistant to tampering (Physical and Access Controls), confidentiality of data in transit (Encryption), and is available for authorized users only (Access Control). Management controls are utilized to prevent the inappropriate disclosure of sensitive information. In addition, the Perimeter Network and Security Infrastructure (NSI) and Enterprise Monitoring And Security Operations (EMSO) provide additional automated transmission and monitoring mechanisms to ensure that PII information is protected and not breached by any outside entities. In the event of disposal, USPTO uses degaussing to permanently remove data according to government mandate and security policy.

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 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

☐	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
☐	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
☒	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 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. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: • Corporate Administrative Office System (CAOS) • Consolidated Financial System (CFS) • Enterprise Software Services (ESS) • Personal Identity verification System Card Management System (HSPD-12/PIVS/CMS) • Information Dissemination Support System (IDSS) • Intellectual Property Leadership Management System (IPLMSS) • Patent Capture and Application Processing System – Examination Support (PCAPS-ES) • Patent Capture and Application Processing System – Capture and Initial Processing (PCAPS-IP) • Patent Search System – Primary Search and Retrieval (PSS-PS) • Patent Search System – Specialized Search and Retrieval (PSS-SS) • Revenue Accounting and Management System (RAM) • Trademark Processing System – External System (TPS-ES) • Trademark Processing System – Internal System (TPS-IS) USPTO uses SC-8, SC-11, SC-12, SC-13 of the NIST System and Communications Protection Control Family to 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.

6.4 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: DSMS houses the data that is stored via other application information systems within USPTO. These other systems provide this functionality for the data that is being stored. DSMS has no authorization to disseminate any type of information since that information is owned by the Application. Each of the systems storing information in DSMS provide individuals with notification on the front-end. DSMS is the enterprise-wide storage solution for USPTO applications. As a result, if PII is collected by an application information system it is that application's responsibility to have the necessary privacy-related notice language.

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:
☒	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: DSMS houses the data that is stored via other application information systems within USPTO. These other systems would provide this functionality for the data that is being stored since that information is owned by the Application.

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:
☒	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: DSMS houses the data that is stored via other application information systems within USPTO. These other systems would provide this functionality for the data that is being stored since that information is owned by the Application.

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: DSMS houses the data that is stored via other application information systems within USPTO. These other systems would provide this functionality for the data that is being stored since that information is owned by the Application.

Section 8: 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. Explanation: Audit Logs are configured to track what has been accessed and when and by whom. These logs are sent to a SEIM which is configured to send an alert to the DSMS team in the case of a particular event being triggered.
☒	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): _10/28/2019_____ ☐ 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 (POA&M).
☒	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
☒	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
☒	Contracts with customers establish DOC 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. *(Include data encryption in transit and/or at rest, if applicable).*

DSMS protects information and retains it within the system according to USPTO requirements and federal law. By default, data is written throughout the set of data drives within the storage array. Since data is located across multiple arrays, it lessens the risk of data loss. There is a different key for each drive in the storage array. The process occurs on the hardware, ensuring there is no possible way to reconstruct the specific data from a pattern of data scripting on multiple drives. Only administrators have access to the information, there are no user accounts on the system.

Restricting boundary traffic to DSMS infrastructure within managed interfaces and prohibiting external malicious traffic are the responsibility of the USPTO network infrastructure. They employ managed interfaces employing boundary protection devices including proxies, gateways, routers, firewalls, guards, or encrypted tunnels arranged in effective security architecture (e.g., routers protecting firewalls and application gateways residing on a protected sub-network referred to as a demilitarized zone or DMZ). This configuration protects the system from basic attacks like tear-drop, syn flood, smurf flood, ping flood and fraggle.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

☐ Yes, the PII/BII is searchable by a personal identifier.

☒ No, the PII/BII is not searchable by a personal identifier.

9.2 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). Provide the SORN name, number, and link. *(list all that apply)*:
☐	Yes, a SORN has been submitted to the Department for approval on (date).
☒	No, this system is not a system of records and a SORN is not applicable. "DSMS simply stores data being used by other applications. Refer to the applications PIAs for details about applicable SORNs."

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. Provide the name of the record control schedule:
☒	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule: "DSMS simply stores data being used by other applications. Refer to the applications PIAs for details about applicable record control schedule."
☐	Yes, retention is monitored for compliance to the schedule.
☒	No, retention is not monitored for compliance to the schedule. Provide explanation: "DSMS simply stores data being used by other applications. Refer to the applications PIAs for details about applicable record control schedule."

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	☐	Overwriting	☒
Degaussing	☐	Deleting	☒
Other (specify): There are periodic back-ups for storage of information			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

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. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

☐	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 level. *(Check all that apply.)*

☒	Identifiability	Provide explanation: The combination of Social Security, Employer ID, Citizenship, File Case ID, Name, Date of Birth, Place of Birth, Home address, Email address, Occupation, Job Title, Work address, Work email, Work phone number, Fingerprints, Photographs, credit card and financial information can be easily used to identify an individual.
☒	Quantity of PII	Provide explanation: DSMS stores large quantities of data that may contain PII from across the USPTO network
☒	Data Field Sensitivity	Provide explanation: The data includes personal and work related elements that include identifying numbers. PII stored in the system is data collected from USTPO HR in which the information is confidential and unique to those individuals.
☒	Context of Use	Provide explanation: Data on DSMS is for backup purposes only.
☒	Obligation to Protect Confidentiality	Provide explanation: Sensitive data is located across different sections of the array and unintelligible without knowledge of all these locations. Since data is located across multiple arrays, it lessens the risk of data loss. As a repository for information from across the USPTO network, DSMS must ensure only authorized systems and individuals have access to their information.
☒	Access to and Location of PII	Provide explanation: Data that may be used, stored, and transmitted by the Application Systems is centrally stored by DSMS. DSMS must ensure that only authorized systems and individuals have access to their data from this central storage system.
☒	Other:	Provide explanation: System applications are responsible for determining the confidentiality impact levels collected, maintained, or disseminated by DSMS.

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

Foreign entities as well as insider threats are the main threats that USPTO has identified. The potential threats to PII could cause a loss of confidentiality and integrity of the information stored on the application.. Based upon USPTO's threat assessment the Agency has implemented base line security controls to mitigate these risks to sensitive information to an acceptable level.

12.2 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. Explanation:
☒	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

☐	Yes, the conduct of this PIA results in required technology changes. Explanation:
☒	No, the conduct of this PIA does not result in any required technology changes.