Template Version Number: 01-2021

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

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

Reviewed by: Deborah Stephens, 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

NICHOLAS CORMIER Digitally signed by NICHOLAS CORMIER Date: 2025.09.17 08:27:55 -04'00' 9/17/2025

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: EIPL-IHSS-01-00

Introduction: System Description

Provide a brief description of the information system.

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

Enterprise Backup Recovery System (EBRS): Provides a consolidated backup system for the entire USPTO. EBRS provides a mechanism to backup and restore data generated and stored on individual servers for disaster recovery purposes. EBRS uses Cohesity Commercial Off the Shelf (COTS) product to provide a reliable backup system. EBRS capabilities include the following:

• Back up data from all servers, regardless of Operating System (OS): USPTO approved OS baselines include Rocky Linux and Windows only.
• Meet the backup timeframe required for each server type.
• Allow administrators to recover data if lost or inadvertently destroyed.
• Recover a server if it crashes or destroys its filesystem contents.

NetApp: The USPTO owned NetApp hosts all of the workstation legacy drives including shared (S:) and home directories (H:). It also hosts shared drives that some products utilize.

Both of these are primarily administered by Computer Services Branch 1 (CSB-1) Storage Administrators and Backup Administrators.

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 Stated Patent and Trademark Office, Alexandria VA.

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

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

Intellectual Property Leadership Management System (IPLMSS) - IPLMSS is an Application Information System that provides capabilities and functionality for patent examiners to perform their roles.

Patent Capture and Application Processing System – Capture and Initial Processing (PCAPS-IP) – provides support to the USPTO for the purposes of capturing patent applications and related metadata in electronic form; processing applications electronically; reporting patent application processing and prosecution status; and retrieving and displaying patent applications.

Patent End to End (PE2E): The purpose of the PE2E 1.0 CRU to provide examination tools for Central examination unit to track and manage the cases in this group and view documents in text format.

Security and Compliance Services (SCS): Provides Security Incident and Event Management, Enterprise Forensic, Enterprise Management System, Security and Defense, Enterprise Scanner, Enterprise Cybersecurity Monitoring Operations, Performance Monitoring Tools, Dynamic Operational Support Plan, & Situational Awareness and Incident Response.

Patent Capture and Application Processing System - Examination Support (PCAPS-ES): The purpose of this system is to process, transmit and store data and images to support the data-capture and conversion requirements of the USPTO to support the USPTO patent application process.

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

Compute Historical Analytics and Reporting Tools (CHART) is a system that is comprised of multiple tools, of which only one is interconnected with DSMS: Data-driven Interconnected Application for Managing Omnifarious Networked Devices (DIAMOND). CHART provides technical, managerial, and financial analyst staff members at United States Patent and Trademark Office (USPTO) with a single, unified view of all host and storage assets managed by the Infrastructure and Hosting Services Division (IHSD) of the Enterprise Infrastructure Delivery Office (EIDO).

Service Management Platform (SMP) is a Software as a Service (SaaS) cloud-based Information Technology Services Management (ITSM) Major Application (MA) that provides a single system of record for IT services, operations, and business management by automating IT service applications and processes.

Corporate Administrative Office System (CAOS) – is an information system that is composed of 3 components Enterprise Telework Information System (ETIS), Record Sharing Platform (RSP) and WebTA that support the Human Resources business functions within the United States Patent and Trademark Office (USPTO).

Patent Business Management Information (PBMI) is a master system portfolio consisting of a collection of Automated Information Systems (AIS) under the Patents product line. The goal of PBMI is to facilitate and support examiner production, quality assurance, and report dissemination to United States Patent and Trademark Office (USPTO) employees and contractors. PBMI provides access to easy-to-acquire validated data and metrics.

International Data Exchange-Moderate (IDE-M) is a system developed by the United States Patent and Trademark Office (USPTO) that help exchange published and unpublished application data with international stakeholders, including foreign intellectual property offices (IPOs) and the World Intellectual Property Organization (WIPO).

Trademark Next Generation (TMNG) is an application information system that provides support for the automated processing of trademark applications for the United States Patent and Trademark Office (USPTO).

Collection of Multiple Enterprise Tools (COMET) is a collection of independent applications that live on ORACLE's Application Express (APEX) lightweight database. COMET provides an USPTO an opportunity to develop minor independent applications for business purposes in an easy and cost-effective manner.

Trademark Processing System – Internal Systems (TPS-IS) is an information system that provides support for the automated processing of trademark applications for the United States Patent and Trademark Office (USPTO). TPS-IS includes four applications that are used to support USPTO staff through the trademark review process.

Trademark Processing System – External Systems (TPS-ES) is a Major Application information system, and provides customer support for processing Trademark applications for USPTO.

Sequencing Listing Information Control (SLIC) is processing system component for Deoxyribonucleic Acid (DNA), Ribonucleic Acid (RNA) & Protein Sequence Listings following ST.23, ST.25 and ST.26 international standards, and in accordance with 37

CFR §§ 1.821 – 1.825 "Application Disclosures Containing Nucleotide and/or Amino Acid Sequences". SLIC will intake sequence listings in ST.23, ST.25 and ST.26 formats, perform compliance verification, provide a workflow for review and data transformation for downstream intake components including Patents Content Management and Patent Search repositories.

Patent Trial and Appeal Case Tracking System (P-TACTS) is an application information system and provides supporting USPTO's administrative law body Patent Trial and Appeal Board for electronically filing documents in connection with the proceedings established under the Leahy-Smith America Invents Act (AIA).

Madrid International Trademark System (MITS) The Madrid International Trademark System assists the Office of Trademark in sending, receiving, reviewing and verifying data from International Bureau (IB)-related to international applications that are being handled by the U.S. Patent and Trademark Office (USPTO) as governed by the Madrid Protocol. The business mission will be enabled through a technical approach of cloud-native infrastructure and DevSecOps pipelines that will enable cost-conscious elastic scalability and quick turnaround time of features and business rule changes utilizing continuous integration and deployment.

Enterprise Management System (EMS) provides for automated, proactive system management, and service-level management for application and database servers. The EMS AIS supports high availability for all the USPTO servers and AIS software including MicroFocus Operations Bridge Manager, Open Network Monitoring Software (OpenNMS), Prometheus, Grafana, and Netdata.

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

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

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.

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.

Patent Search System – Specialized Search and Retrieval (PSS-SS) is a major application that provides access to specialized data that may include annual submissions of nucleic and amino acid sequence or prior-art searching of polynucleotide and polypeptide sequences, and other types of information that may be more scientific or the technology-based, Patent Linguistic Utility Service (a query by example search system), Chemical Drawing ability, and Foreign Patent Data. The PSS-SS system is made up of three applications that allow patent examiners and applicants to effectively search the USPTO Patent data repositories.

Cooperative Patent Classification (CPC) provides tools to apply allocations and a master database that serves as the authoritative source for allocations placed by the USPTO, European Patent Office (EPO) and other offices.

(d) The way the system operates to achieve the purpose(s) identified in Section 4

DSMS is the hosting environment that EBRS and NetApp applications use to provide archive and storage capabilities to USPTO users.

(e) How information in the system is retrieved by the user

The information in the system is retrieved by authorized users 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 Storage Area Network (SAN) Switches and Routers.

(g) Any information sharing

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

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.

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 DSMS system acts as a backup storage application for many systems within USPTO, some of which collect SSN. Please refer to the PIA, for the interconnections listed in Section C of the introduction.					

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. Marital Status	☐
f. Race/Ethnicity	☐	m. Education	☐	t. Mother's Maiden Name	☐
g. Citizenship	☐	n. Religion	☐		

u. Other general personal data (specify): DSMS only provides backup services for all on-prem systems managed by CSB-1 for system recovery purposes. The data stored within DSMS is not visible by DSMS Administrators and is based on the application or product that use DSMS for its storage and recovery capabilities. Please refer to the PIA for the interconnections listed in section c of the introduction for their need to collect, maintain and disseminate PII such SSNs.

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):
DSMS only provides backup services for all on-prem systems managed by Compute Services Branch 1 (CSB-1) for system recovery purposes. The data stored within DSMS is not visible by DSMS Administrators and is based on the application or product that use DSMS for its storage and recovery capabilities. Please refer to the PIA for the interconnections listed in section c of the introduction for their need to collect, maintain and disseminate PII such SSNs.

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):
DSMS provides backup services for all on-prem systems managed by CSB-1 These on-prem systems may choose to change their PII collected at any time as they are the owners of their PII information. To see the PII collected by these systems, please refer to the PIA for the interconnections listed in Section C.

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): The DSMS system has the capability and function to collect audit data for components it uses such as Cohesity.

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): DSMS provides backup services for all on-prem systems managed by CSB-1. These on-prem systems may change how they ingest PII collected at any time as they are the owners of their PII information. To see the PII collected by these systems, please refer to the PIA for the interconnections listed in section c.					

Government Sources					
Within the Bureau	☒	Other DOC Bureaus	☐	Other Federal Agencies	☐
State, Local, Tribal	☐	Foreign	☐		
Other (specify): DSMS provides backup services for all on-prem systems managed by CSB-1. These on-prem systems may change how they ingest PII collected at any time as they are the owners of their PII information. To see the PII collected by these systems, please refer to the PIA for the interconnections listed in section c.					

Non-government Sources					
Public Organizations	☐	Private Sector	☐	Commercial Data Brokers	☐
Third Party Website or Application			☐		
Other (specify): DSMS provides backup services for all on-prem systems managed by CSB-1. These on-prem systems may change how they ingest PII collected at any time as they are the owners of their PII information. To see the PII collected by these systems, please refer to the PIA for the interconnections listed in section c.					

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

For the audit data that the DSMS system collects, access control restrictions are in place and principle of least privilege in maintained to ensure only authorized individuals have access to audit log files.

The system is secured using appropriate administrative physical and technical safeguards in accordance with the National Institute of Standards and Technology (NIST) security controls (encryption, access control, and auditing). Mandatory Information Technology (IT) awareness and role-based training is required for staff who have access to the system and address how to handle, retain, and dispose of data. All access has role-based restrictions and individuals with privileges have undergone vetting and suitability screening. The USPTO

maintains an audit trail and performs random, periodic reviews (quarterly) to identify unauthorized access and changes as part of verifying the integrity of administrative account holder data and roles. Inactive accounts will be deactivated and roles will be deleted from the application. Additionally, DSMS only provides backup services for all on-prem systems managed by CSB-1 for system recovery purposes. The data stored within DSMS is not visible by DSMS Administrators and is based on the application or product that use DSMS for its storage and recovery capabilities. The DSMS Administrators only manage the server backups or restore data as needed by the product teams. To determine how accuracy of the information in the system is ensured please refer to the PIA for the interconnections listed in section c of the introduction.

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): Click or tap here to enter text.			

☒	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): DSMS purpose is to provide backup services for all on-prem systems managed by CSB-1 for system recovery.			

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 provides backup services for all on-prem systems managed by CSB-1. These on-prem systems may choose to change their PII collected at any time as they are the owners of their PII information. To see the PII collected by these systems, please refer to the PIA for the interconnections listed in section c.

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.)

In the event of computer failure, insider threats, or attack against the system by adversarial or foreign entities, any potential PII data stored within the system could be exposed. To avoid a breach, the system has certain security controls in place to ensure the information is handled, retained, and disposed of appropriately. Access to individual's PII is controlled through the application, and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. These audit trails are based on application server out-of-the-box logging reports reviewed by the Information System Security Officer (ISSO) and System Auditor and any suspicious indicators such as browsing will be immediately investigated and appropriate action taken. Also, system users undergo annual mandatory training regarding appropriate handling of information.

NIST security controls are in place to ensure that information is handled, retained, and disposed of appropriately. For example, advanced encryption is used to secure the data both during transmission and while stored at rest. Access to individual's PII is controlled through the application and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. USPTO requires annual security role based training and annual mandatory security awareness procedure training for all employees. All offices of the USPTO adhere to the USPTO Records Management Office's Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citation.

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): DSMS only provides backup services for all on-prem servers and systems managed by CSB-1 for system recovery purposes. Please refer to the PIA for the interconnections listed in section c of the introduction.	☒	☒	☐

☐	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: IPLMSS PCAPS-IP PE2E SCS PCAPS-ES CAOS PBMI IDE-M TMNG COMET TPS-IS TPS-ES PTACTS MITS ID-AUTH ESS PSS-SS SMP NIST security controls are in place to ensure that information is handled, retained, and disposed of appropriately. For example, advanced encryption is used to secure the data both during transmission and while stored at rest. Access to individual's PII is controlled through the application and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. USPTO requires annual security role based training and annual mandatory security awareness procedure training for all employees. All offices of the USPTO adhere to the USPTO Records Management Office's Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citation.
☐	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): DSMS provides backup services for all on-prem systems managed by CSB-1. These on-prem systems may choose to change their PII collected at any time as they are the owners of their PII information. To see the PII collected by these systems, please refer to the PIA for the interconnections listed in section c.			

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: https://www.uspto.gov/privacy-policy	
☐	Yes, notice is provided by other means.	Specify how:
☒	No, notice is not provided.	Specify why not: DSMS only provides backup services for all on-prem systems managed by CSB-1 for system recovery purposes. The data stored within DSMS is not visible by DSMS Administrators and is based on the application or product that use DSMS for its storage and recovery capabilities. DSMS has no authorization to disseminate any type of information since that information is owned by the Application. If PII is collected by an application information system it is that application's responsibility to have the necessary privacy-related notice language. Please refer to the PIA for the interconnections listed in section c of the introduction.

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 only provides backup services for all on-prem systems managed by CSB-1 for system recovery purposes. These systems would provide this functionality for the data that is being stored since that information is owned by the Application. DSMS does not provide individuals the opportunity to decline to provide PII/BII. Please refer to the PIA for the interconnections listed in section c of the introduction.

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 only provides backup services for all on-prem systems managed by CSB-1 for system recovery purposes. These systems would provide this functionality for the data that is being stored since that information is owned by the Application. If PII is collected by an information system, that system would provide determine if an individual has an opportunity to consent to particular uses of their PII/BII. Please refer to the PIA for the interconnections listed in section c of the introduction.

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 only provides backup services for all on-prem systems managed by CSB-1 for system recovery purposes. These other systems would provide this functionality for the data that is being stored since that information is owned by the Application. If PII is collected by an information system, that system would provide determine if an individual has an opportunity to consent to particular uses of their PII/BII. Please refer to the PIA for the interconnections listed in section c of the introduction.

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: DSMS audit Logs are configured to track what has been accessed and when and by whom. These logs are sent to a Security Information and Event Management (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): 3/12/2025

	☐ 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 5 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): Please refer to the PIA for the interconnections listed in section c of the introduction.

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).*

PII within the system is secured using appropriate management, operational, and technical safeguards in accordance with NIST requirements. Such management controls include a review process to ensure that management controls are in place and documented in the System Security Privacy Plan (SSPP). The SSPP specifically addresses the management, operational, and technical controls that are in place and planned during the operation of the system. Operational safeguards include restricting access to PII/BII data to a small subset of users. 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 system maintains an audit trail and the appropriate personnel is alerted when there is suspicious activity. Data is encrypted in transit and at rest.

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. The systems that DSMS provides back-up for may collect PII and/or BII and have it backed-up in DSMS. The information for these back-ups is not searchable in DSMS. Please refer to the PIA for the interconnections listed in section c of the introduction 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.)*

General Records Schedules (GRS) | National Archives

☐	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: The systems that DSMS provides back-up for may collect PII and/or BII and have it backed-up in DSMS. The information for these back-ups is not searchable in DSMS. Please refer to the PIA for the interconnections listed in section c of the introduction for details about applicable record control schedules that are maintained by these systems.
☐	Yes, retention is monitored for compliance to the schedule.
☐	No, retention is not monitored for compliance to the schedule. Provide explanation:

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

Disposal			
Shredding	☐	Overwriting	☐
Degaussing	☐	Deleting	☐
Other (specify): DSMS only provides backup services for all on-prem systems managed by CSB-1 for system recovery purposes. The data stored within DSMS is not visible by DSMS Administrators and is based on the application or product that use DSMS for its storage and recovery capabilities. Please refer to the PIA for the interconnections listed in section c of the introduction about PII/BII disposal methods.			

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 data from different sources and systems within the USPTO environment that contain PII or BII information.
☒	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 the USPTO system it interconnects with in which the information is confidential and unique to those systems.
☒	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: DSMS only provides backup services for all on-prem systems managed by CSB-1 for system recovery purposes. System applications are responsible for determining the confidentiality impact levels collected, maintained, or disseminated by their applications. Please refer to the PIA for the interconnections listed in section c of the introduction.

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.)

The PII in this system poses a risk if exposed. System users undergo annual mandatory training regarding appropriate handling of information. Physical access to servers is restricted to only a few authorized individuals. The servers storing the potential PII are located in a highly sensitive zone within the cloud and logical access is segregated with network firewalls and switches through an Access Control list that limits access to only a few approved and authorized accounts. USPTO monitors, in real-time, all activities and events within the servers storing the potential PII data and personnel review audit logs received on a regular bases and alert the appropriate personnel when inappropriate or unusual activity is identified.

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.