Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
Open Data-Big Data Master System (OD-BD MS)

Reviewed by: Jamie Holcombe

▣ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

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

CHARLES CUTSHALL Digitally signed by CHARLES CUTSHALL
Date: 2025.02.20 15:15:06 -05'00' 2/20/2025

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO Open Data-Big Data Master System (OD-BD MS)

Unique Project Identifier: PTOC-034-00

Introduction: System Description

Provide a brief description of the information system.

The Open Data/Big Data master system (OD-BD MS) consists of subsystems which support the Big Data Portfolio.

Big Data Reservoir (BDR):
The BDR is a subsystem of OD-BD MS used by United States Patent and Trademark Office (USPTO) employees. Employees used BDR to analyze structured and unstructured data utilizing data science best practices to improve USPTO business for USPTO customers.

BDR collects and ingests information across USPTO. BDR takes that information and consolidates both unstructured data sources or data sources that have evolved into multiple structures over time. Where possible, BDR provides a web view for USPTO examiners to view aggregated information relevant to their work. Additionally, BDR analytics can be used at various levels of management within USPTO through simplified yet insightful reporting for advanced analytics.

Bulk Data Storage System (BDSS):
The BDSS Application Program Interface (API) is used to support full-text and field specific searches related to bulk data products. Bulk Data products include only public and disseminable patent and trademark data in the form of zip files. BDSS provides the public with alternative methods to access bulk data products on https://bulkdata.uspto.gov.

Developer Hub (DH):
DH provides the general public and the developer community a place to consume USPTO information in a bulk data format. DH provides the public accessible, discoverable, and usable USPTO data through a user interface and Web Services Application Programming Interfaces (API). The aim of DH is to promote development of new data products, analytics and services while at the same time meeting USPTOs commitment to building a 21st Century Digital Government[3].

DH provides developers public data about patents, trademarks and events.

Consolidation of Economic Analysis Tools (COEAT):
COEAT is used to store data and preform statistical analysis in a secured environment by the USPTO's Chief Economist's office. COEAT includes hundreds of statistical tools and many data-management commands that provide complete control of all types of data that include byte, integers, long, float, double, and string variables. COEAT generates publication-quality, distinctly styled graphs using an integrated graph editor to ensure that no unauthorized users access the system

Developer Hub Assignment Search (DH-AS):

[3] Federal Register :: Building a 21st Century Digital Government

The Assignment Search application is a search tool to allow external users to search and track changes in ownership to a patent or trademark property.

Address the following elements:

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

OD-BD MS is a major application which employs IaaS and PaaS services from USPTO's AWS.

(b) System location

Manassas, Virginia and AWS East/West

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

OD-BD MS interconnects to:

Information Dissemination Support System (IDSS): supports the Trademark and Electronic Government Business Division, the Corporate Systems Division (CSD), the Patent Search System Division, the Office of Electronic Information Products, and the Office of Public Information Services.

Identity, Credential, and Access Management - Identity as a Service (ICAM-IDaaS) - provides Single Sign-On capabilities to BDR.

Patent Capture and Application Processing System-PCAPS-Examination Support (PCAPS-ES) – processes, transmits and stores data and images to support the data-capture and conversion requirements of the USPTO to support the USPTO patent application process.

Enterprise Software Service (ESS): provides COMET the active directory to facilitate access management. ESS provides USPTO with a collection of programs that utilize common business applications and tools for modeling how the entire organization works. ESS provides a centralized solution for assisting developers in building applications unique to the organization.

Network and Security Infrastructure System (NSI) - is an Infrastructure information system, and provides an aggregate of subsystems that facilitates the communications, secure access, protective services, and network infrastructure support for all USPTO IT applications.

Enterprise UNIX Services (EUS) - consists of assorted UNIX operating system (OS) variants, each comprised of many utilities along with the master control program, the kernel.

Enterprise Windows Servers (EWS) - is an Infrastructure information system, and provides a hosting platform for major applications that support various USPTO missions.

Database Services (DBS) - is an Infrastructure information system, and provides a Database Infrastructure to support the mission of USPTO database needs.

Data Storage Management System (DSMS) - provides a secure environment for archival and storage of data and records vital to USPTO's Business Continuity and Disaster Recovery plan.

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

Patent Capture Application Processing System – Initial Processing (PCAPS-IP) - captures patent applications and related metadata in electronic form; processing applications electronically; reporting patent application processing and prosecution status; and retrieving and displaying patent applications. PCAPS-IP is comprised of multiple Automated Information Systems (components) that perform specific functions, including submissions, categorization, metadata capture, and patent examiner assignment of patent applications.

Trademark Processing System – Internal System (TPS-IS) - provides support for the automated processing of trademark applications for the USPTO. TPS-IS includes eleven applications that are used to support USPTO staff through the trademark review process.

Patent End to End (PE2E) - provides examination tools for Central examination unit to track and manage the cases in this group and view documents in text format.

Trademark Next Generation (TMNG) - provides support for the automated processing of trademark applications for the USPTO.

Patent Trial and Appeal Case Tracking System (P-TACTS) - is used for electronically filing documents in connection with Inter Parties Review (IPR), Covered Business Method Patents (CBM), Post Grant Review (PGR), and Derivation Proceedings (DER) established under the Leahy-Smith America Invents Act (AIA).

Patent Public Search (PPUBS) - allows public users to search for patent information used during examination to make patentability determinations.

Enterprise Management System (EMS) - provides automated, proactive system and service-level management of network, office automation, and application servers operating within the USPTO PTOnet environment.

USPTO Amazon Web Services Cloud Services (UACS) - is the infrastructure-as-a-Service (IaaS) platform used to support USPTO Application Information Systems (AIS) hosted in the Amazon Web Services (AWS) East/West environment.

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

BDR: The BDR application provides a platform for data scientists to perform advanced analytics on various data sets that support the agency's customers. BDR contains multiple data sources within the USPTO to support the creation of statistical models and data visualizations to gather insight into the agency's data and strategic planning.

BDSS: A member of the public can visit access BDSS on https://bulkdata.uspto.gov. From there individuals are able to select what types of data they would like to download such as various types of patent information (Patent Official Gazettes,[4] Patent Grant information, Published Patent Applications and additional patent information), trademark information (application and registration images, trademark text), and research datasets over various years. Once downloaded the individual is able to view the information outside of USPTO system and further analyze or process the information as they see fit.

DH: A member of the public can access DH on USPTOs website. From there individuals are able to explore the data available, view USPTOs available APIs or view our findings. An individual can navigate through the site just like any other website, through a search button or navigating with DH to view APIs, web analytics, datasets and visualizations.

COEAT: The COEAT application supports the sharing of analytic and data themes used in the production of business intelligence and advanced analytical solutions. COEAT supports the research mission of the Office of the Chief Economist (OCE).

DH-AS: The application provides external customers with assignment information through advanced search functionality as it relates to the ownership to a patent or trademark.

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

[4] Official Gazette | USPTO

BDR is a large repository for structures and unstructured data. There is the compute tier, where the data is loaded, compared for public versus private status, and analyzed according to data science principles. There is the analysis tier, where data scientists combine the real-world problem-solving techniques from Patent Examiners with the formulae and hypothesis of the Data Science field. The visualization tier that provides the users with a place to view the analysis and the underlying data that helps to create it. Finally, in the storage tier, the system retains raw, merged and transformed data, disseminates between public and privacy Patent applications and segregates them. Dashboards, search functionality, and visualizations provide users the ability to view the BDR data.

BDSS: Information is retrieved by the public over the internet, no login is required.

COEAT: The COEAT users can access the data contents within the USPTO network. In order to access COEAT data, the users connect over SSH to the COEAT server.

DH: Public users have access to a web portal to query Patents and Trademarks data.

DH-AS: Users retrieve Patent data from DH-AS over the internet via a webpage.

(f) How information is transmitted to and from the system

BDR: Information is transmitted through batches, service calls (Databricks), and user entry (BDR-TQR feature). All transmissions and retrieval of information are performed within the USPTO network and do not exceed the internal network boundary.

The BDR application employs a multilayered design approach. This approach gives modularity to the system. The following sections explain in high level, how each layer is comprised. The design principle of the BDR aims to have a tiered approach to the application. This way every component of the ecosystem is more easily understood and viewed independently. In this platform, there is ingestion, where the data is ingested from existing software resources. There is the compute tier, where the data is loaded, compared for public versus private status, and analyzed according to data science principles. There is the analysis tier, where data scientists combine the real-world problem-solving techniques from Patent Examiners with the formulae and hypothesis of the Data Science field. The Visualization tier that provides the users with a place to view the analysis and the underlying data that helps to create it. Finally, in the storage tier, the system retains raw, merged and transformed data, distinguishes between public and private Patent applications, and segregates them.

DH:

The DH system provides USPTO public data (such as patents, trademarks, and events data) via a set of Web Services APIs for the consumption of the developer community. These APIs will be developed and maintained by various divisions within USPTO and will be accessible through a USPTO web UI named Developer Hub, or Davent Hub System Name. The system provides access to USPTO public content through the use of APIs (application programming interface). The DH web application is deployed on the Amazon Web Services (AWS) Cloud platform. Users include: General Public, System Development Staff, Tableau Public Users, EC2 Server Accounts, Drupal Admin User via RBAC, and System Administrators.

COEAT: The data within COEAT is ingested from BDSS, CEDR-INFRA, EDW and PEDS via HTTPS and Direct Database Access

BDSS: The data from BDSS is ingested from internal and external sources over Secure File Transfer Protocol (SFTP) and Hypertext Transfer Protocol Secure (HTTPS).

DH-AS: Information is transmitted to and from DH internally over HTTPS.

(g) Any information sharing

BDR: Information is only shared within USPTO to BDSS, DH and PSAI.

BDSS: All information is available to the public and does not require a login to access the system.

COEAT: Information is shared only within USPTO, COEAT ingests data from BDSS, Central Enterprise Data Repository Infrastructure (CEDR-INFRA), Enterprise Data Warehouse (EDW) and Patent Examination Data Search (PEDS)

DH: All information is available to the public and does not require a login to access the system.

DH-AS: All information is available to the public and does not require a login to access the system.

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

35 U.S.C. 1, 2, 6, 23, 24, 115, and 135
15 U.S.C 1051-1141n
5 U.S.C. 301
Building a 21st Century Digital Government
Code of Federal Regulations Title 37,

(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): TEAS Application ID/Serial Number/Registration Number for specific Trademarks. Serial Number/Registration Number is used by applicants to track progress of Trademark Applications. Patent application number and granted Patent number					

*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:

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):					

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): Pre-published patent applications and Trademark Office Actions					

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):					

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.

The accuracy of the information in the system is ensured by receiving the information from systems that obtained the information directly from the individual. For transferring the data appropriate checks are put in place to ensure the integrity of the data transferred between the interconnections. 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 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.

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. 0651-0063 Patent Trial and Appeal Board 0651-0040 Trademark Trial and Appeal Board

	0651-0032 Initial Patent Applications 0651-0009 Applications for Trademark Registration
□	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): To perform advanced analytics to identify patterns and trends.			

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).

BDR

Who the PII is referencing	PII/BII identified in Section 2.1	How the information will be used
Member of the public: Yes	Employee ID, Name, Email Address, User ID	The information will be used for Authentication and Data Visualization
USPTO employee or contractor:		

COEAT

Who the PII is referencing	PII/BII identified in Section 2.1	How the information will be used
Member of the public: Yes	Name, Gender, Citizenship, Home Address, Work Address, Business Information, Employee ID, Race/Ethnicity.	This information will be used to track inventors and trademark owners.

USPTO employee or contractor:		

BDSS

Who the PII is referencing	PII/BII identified in Section 2.1	How the information will be used
Member of the public: Yes	Name, Citizenship, Home Address, Work Address, Work Telephone Number, Work Email Address, Business Information.	The information will be used for Data Visualization and Storage.
USPTO employee or contractor:		

DH

Who the PII is referencing	PII/BII identified in Section 2.1	How the information will be used
Member of the public: Yes	Name, Citizenship, Home Address, Work Address, Work Telephone Number, Work Email Address, Business Information	The information will be used for Data Visualization.
USPTO employee or contractor:		

DH-AS

Who the PII is referencing	PII/BII identified in Section 2.1	How the information will be used
Member of the public: Yes	Name, Work Address, Home Address, Work Telephone Number, Work Email Address, Business Information.	The information will be provided to end users who are performing assignment searches.
USPTO employee or contractor:		

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):	□	□	□

□	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 infomation 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: ICAM-IDaaS IDE-M P-TACTS PCAPS-ES TMNG 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): Publicly available PII/BII data is shared through dissemination, non-public PII/BII is only accessible internally			

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:

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: Individuals do not have the opportunity to decline to provide PII/BII with OD-BDMS, that opportunity would be determined by whichever system the individual originally provided the data.

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: Individuals do not have the opportunity to consent to particular uses of their PII/BII with OD-BDMS, that opportunity would be determined by whichever system the individual originally provided the data.

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: Individuals do not have the opportunity to review or update their PII/BII with OD-BDMS, that opportunity would be determined by whichever system the individual originally provided the data.

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

☒	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): 5/24/2024 ☐ 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 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): All users (end-users and administrators) are explicitly authorized to have access to the data processed within BDR. Users are granted access on a need-to-know basis, and RBAC is employed to ensure that only users with the appropriate roles have access to certain functionality/views within the system.

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)*: COMMERCE/PAT-TM-6: Parties Involved in Patent Interference Proceedings COMMERCE/PAT-TM-7: Patent Application Files COMMERCE/USPTO-26: Trademark Application and Registration Records
☐	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.

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: General Records Schedule 5.1, item 020
☐	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:
☒	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): ODBD systems do not handle physical copies of PII/BII. There is no need for shredding.			

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: Name, home address, work address, work email, work phone number can all be used to identify an individual.
☒	Quantity of PII	Provide explanation: Collectively, the number of records maintained generate an enormous amount of PII and a breach in such large numbers of individual PII must be considered in the determination of the impact level. There are about 3 million PII related records specific to the TEAS data.
☒	Data Field Sensitivity	Provide explanation: The data includes limited personal and work related elements and does not include sensitive PII.
☒	Context of Use	Provide explanation: The data is used extensively within the Trademarks Data and Analytics team only. There will be no dissemination of this data any further.
☒	Obligation to Protect Confidentiality	Provide explanation: Based on the data fields and in accordance with the Privacy Act of 1974, PII must be protected.
☒	Access to and Location of PII	Provide explanation: All the TEAS data being ingested will stay within the BDR boundary
☒	Other:	Provide explanation: A lot of PII data associated with TEAS applications have historically been made available to the public. The change to mask the PII data has gone/will go into effect soon (Timeline to be determined by Office of Trademarks).

<u>Section 12</u>: 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.