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: 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

Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry
Date: 2024.02.02 11:08:41 -05'00'

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

Big Data Reservoir (BDR):
The BDR provides the United States Patent and Trademark Office (USPTO) employees a Big Data platform in which they can view records and associated metadata in one location. The BDR uses a fault-tolerant data storage file system called Hadoop Distributed File System (HDFS) infrastructure to perform advanced analytics on unalike and distinctly different data sets consisting of structured and unstructured data in order to gain insights and develop models. System users are USPTO Internal Users. BDR is a large repository for structured and unstructured data. Models and algorithms are developed with the BDR data to provide insights to USPTO executives. Dashboards, search functionality, and visualizations provide users the ability to view the BDR data.

BDR-Trademark Quality Review (TQR):
In addition to the BDR Portal, the BDR also provides the TQR Portal. The TQR Portal provides quality reviewers with a centralized location to view the Dockets that are in the queue for review and additional features that include reviewing Trademark Review forms and completing necessary actions, final and non-final. System users are USPTO Internal Users.

BDR-Cooperative Patent Classification (CPC):
CPC is used to automatically classify patent documents. Users can input .csv files by using Secure File Transfer Protocol (SFTP), which contains a number of application IDs. By using this input file, BDR AI API gets the contractor data from the CPC OracleDB and machine data from the BDR AI for corresponding application IDs and stores the data in two csv files. Users can compare contractor data and machine data, by giving application ID in the WEB. System users are USPTO Internal Users.

BDR-Patent Trial and Appeal Board (PTAB):
PTAB uses the BDR framework to gather data from the PTAB End to End (E2E) Oracle DB (PALMGP) and from two of the One Patent Service Gateway (OPSG) REST APIs. Newly populated data in Oracle DB is collected and stored in BDR using techniques to provide structure to the data. The entire table's data is stored in SOLR index (Public), Elastic Index, and users can easily search the data based on a particular attribute. System users are USPTO Internal Users.

Address the following elements:

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

OD-BD is a major application.

(b) *System location*
OD-BD resides on the USPTO AWS Cloud Service (UACS) and is located in AWS IaaS East Region.

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

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.

Trademark Processing System – External System (TPS ES): Provides customer support for processing Trademark applications for USPTO.

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.

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 Capture and Application Processing System – 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.

Patent Capture and Application Processing System – Capture and 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.

Enterprise Software Services (ESS): 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.

(d) The way the system operates to achieve the purpose(s) identified in Section 4
BDR is a large repository for structured and unstructured data. Models and algorithms are developed with the BDR data to provide insights to PTO executives. Dashboards, search functionality, and visualizations provide users the ability to view the BDR data.

(e) How information in the system is retrieved by the user
BDR is a large repository for structured 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 private Patent applications and segregates them. Dashboards, search functionality, and visualizations provide users the ability to view the BDR data.
DH uses an N-tier architectural design pattern that separates the processing logic into distinct processing layers. The system is logically divided into six major subsystems:

- **Access Layer**: The access layer includes client web browsers and applications. Browser-based users can access DH web front and its contents. Users can also view DS-API Swagger pages and perform searches on data for various data sets.
- **Web Server Layer**: This layer hosts Apache Web servers. To follow USPTO EA standards, Apache is configured as the web server in front of the Wildfly server. The Web Server layer serves two purposes—presenting DH's static and dynamic content, and receiving and responding to DS- API web services calls (HTTP Get/Post messages). The Application Load Balancer routes the web services calls to Wildfly, which hosts the DS-API Web services. Apache Web Server is the server and uses AWS Elastic Load Balancing (ELB) for load balancing applications.
- **Application Server Layer:** This layer uses Wildfly application server to host various Springboot Web Services such as user authentication, email subscription / notification, ETL process and data synchronization. The Wildfly servers are configured in cluster; if a server goes down, subsequent user requests can be forwarded to a different server.
- **Search Layer:** In BDR, we are utilizing ElasticSearch to provide search capabilities against various data-sets. In DH, we are using SolrCloud to provide the same search capabilities.
- **Data Layer:** The Data Layer is responsible for providing access to the data from various sources, such as Drupal Relational Database (RDS), DS- API Relational Database (RDS), Unstructured Events Data (AWS S3).
- **Infrastructure Layer**: This layer provides user registration, authentication and authorization using Okta.

The DH Assignment Search (DH-AS) system indexes patent assignment records and allows them to be searchable by the public. To accomplish this, the system writes the internal records as files and transfers them to a receiving file system. A process monitors this file system and sends the records to the search system for indexing. Once complete with indexing, the whole file is transferred to another file system. If any errors occur, a third file system receives the file.

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

BDR: Information is transmitted through batches, service calls, 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.

Developer Hub (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 DH System Name.

The system provides access to USPTO public content through the use of APIs (application programming interface). It has been determined that DH does not process PII/BII information, and it is categorized as a low-risk system. 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.

Developer Hub Assignment Search (DH-AS): DH-AS is responsible for indexing patent and trademark assignment records, which allows them to be searched by the public. To accomplish this, the internal records are written as files and transferred from AHD to a receiving file system. DH-AS is hosted on an AWS Public Cloud using the IaaS Service Model. It has been determined that DH-AS does not process PII/BII information, and it is categorized as a low-risk system. The DH web application is deployed on the Amazon Web Services (AWS) Cloud platform. Users include: PTONet internal users - Assignment Historical Database (AHD), Assignment Services Branch, USPTO personnel such as patent examiners and support staff, Public Search Facilities staff members, and SOLR administrators.

AS provides public access via Amazon's Web Service Cloud the capability for external users of the USPTO as well as public users in the USPTO public search rooms (with access to the Internet) to query issued patent or published application patent assignment data and/or pending or registered trademark assignment data. The AS web application is deployed to the middleware environment running under Apache web servers and is available to external customers/users of the USPTO (outside of PTONet) via the Internet.

(g) Any information sharing

The BDR system has two operations. First, the data from multiple streams is extracted from the existing resources, including PALMGP, PEDS, PATI/PATI-CDC and P-ELP. Second, the BDR system will load all of these raw data values into the BDR HDFS system, which will then in turn store all of the values into Hive clusters.

BDR-TQR ingestion tier includes existing USPTO data sources, HDFS and Hive Tables and the NiFi schedule. In this tier, the BDR system has two operations. First, the data from multiple streams is extracted from the existing resources, including FAST2 and TRM. Second, the BDR system will load all of these raw data values into the BDR HDFS system, which will then in turn store all of the values into Hive clusters. These clusters act as databases that will store millions of records and our accessible to the other tiers.

BDR-PTAB ingestion tier includes existing USPTO data sources, HDFS and Hive Tables and the NiFi schedule. In this tier, the BDR system has two operations. First, the data from multiple streams is extracted from the existing resources, including PTABE2E (Oracle DB) and Alfresco Systems. Second, the BDR system will load all of these raw data values into the BDR HDFS system, which will then in turn store all of the values into Hive clusters. These clusters act as databases that will store millions of records and our accessible to the other tiers.

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

35 USC 2(b), 6, 115 and 15 USC 1051, 1067, 1070.

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

OD-BD is a Moderate System.

<u>Section 1</u>: 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.					
*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): TEAS collects home address to ascertain domicile of the applicant.					

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): No distinguishing features/biometrics are collected/stored in BDR.					

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)
BII: Information related to pre-published patent applications and Trademark Office Actions.

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): Information Systems internal to USPTO					

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 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
□	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): BII: To perform advanced analytics to identify patterns and trends in an internal USPTO system. Data is used for analysis only and not transferred to any other USPTO/external system.			

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).

PII in BDR is ingested from TEAS system, which is the authoritative source. This PII is related to members of the general public that apply for Trademarks with the USPTO.

The BII refers to the inclusion of pre-published patent applications and correspondence related to those applications. Other BII consists of Trademark Office Action Data. This BII data is collected from their authoritative sources from their respective information systems from disparate data sets and ingested into the BDR for visualization and modeling.

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 attach 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 adhere to the USPTO Records Management Office's Comprehensive Records Schedule or the General Records Schedule and the corresponding disposition authorities or citations.

Insider threats and foreign entities are the main threats to the system. The potential danger in the BII being compromised is the potential for sharing of information that is required to be held in confidence for a specified period of time per statute and regulation, e.g., 35 USC 122 and 37 CFR 1.211. All end-users and administrators of the BDR system have a valid need-to-know access to the system, and undergo the USPTO Annual IT Security Awareness Training provided by the agency. This training covers proper information handling, retention, and disposal at an enterprise level, which is applicable to all information systems to include BDR.

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): congress (as requested)	☒	□	□

□	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: IDSS TPS-ES PE2E TMNG TPS-IS PCAPS-ES PCAPS-IP ESS

	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 adhere to the USPTO Records Management Office's Comprehensive Records Schedule or the General Records Schedule and the corresponding disposition authorities or citations. Insider threats and foreign entities are the main threats to the system. The potential danger in the BII being compromised is the potential for sharing of information that is required to be held in confidence for a specified period of time per statute and regulation, e.g., 35 USC 122 and 37 CFR 1.211. All end-users and administrators of the BDR system have a valid need-to-know access to the system, and undergo the USPTO Annual IT Security Awareness Training provided by the agency. This training covers proper information handling, retention, and disposal at an enterprise level, which is applicable to all information systems to include BDR.
☐	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: This PIA serves as notice.

☐	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: Not applicable. Data is copied from an existing PTO authoritative source system.

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: Not applicable. Data is copied from an existing PTO authoritative source system.

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: Not applicable. Data is copied from an existing PTO authoritative source system.

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: Role based access to the BDR portal controlled through the PTO RBAC system. User access to the system is also tracked through 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): 5/23/2023

	□ 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): 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).*

Data encryption in transit via TLS 1.2. Options for secure data upload/download and encryption of data at rest are provided for additional data protection. Role-based access control and access only granted to a limited number of users are used to protect PII/BII.

<u>Section 9</u>: 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/PAT-TM-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.)*

☒	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):			

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: OD-BD is a cloud-based system with limited access.
□	Other:	Provide explanation:

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.)

BDR resides in USPTO East production environment. Access to the BDR is very limited and controlled by the BDR PM team. IDM accounts must be created by Operations for new accounts requested by members of the BDR PM team. Data is protected in transit through TLS 1.2. Administrative access to the back-end is limited to trusted individuals on the development team. Access is controlled to the BDR portal through RBAC enforcement. The correspondence related to non-published applications are made public when the application is made public (typically after a period of 18 months). Given the limited access and the limited amount of data falling under this category, the threat of BII leakage is very low. Access to the user interface is not exposed to the public internet and only kept internally within the USPTO network.

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.