Version Number: 02-2018

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

Privacy Impact Assessment
for the
Database Services (DBS)

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

CATRINA PURVIS

Digitally signed by CATRINA PURVIS
Date: 2019.09.23 18:41:21 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO Database Services (DBS)

Unique Project Identifier: PTOI-026-00

Introduction: System Description

The DBS is a general support system for databases at USPTO. It is internally hosted at USPTO's Datacenter located at 600 Dulany St, Alexandria, VA 22314 in the Madison East Building. Database systems are comprised of multiple instances of the application, along with data storage. An instance consists of a set of operating-system processes and memory structures that interact with the storage. Data is stored logically in the form of table spaces and physically in the form of data files. The Database Services Branch (DSB) manages and maintains database management software installed on enterprise and application servers. They perform database control and administration functions associated with database operations, performance, and integrity. Support services are also provided for developing Automated Information Systems (AISs) such as requirements analysis, database design, and implementation and maintenance strategies of database applications.

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

(a) a general description of the information in the system
Database Services (DBS) is a supporting information system, and provides a Database infrastructure to support the mission of USPTO Database needs. The DBS System is composed of a collection of various versions of Database systems. The subsystems within the DBS System are:

- Microsoft SQL Database Servers (MSSQL)
- Oracle (Oracle)
- MySQL (MySQL)

(b) a description of a typical transaction conducted on the system
Data is not collected by the DBS system. Data is collected by USPTO systems and stored in database instances. The system that houses the instances is managed by the DBS system. There is a variety of information stored in databases that utilize the DBS software.

(c) any information sharing conducted by the system
The information is shared through the AIS and is not controlled by the DBS system. Information is shared through a web service or front-end system through another interface which is a separately accredited system. The information is shared with financial organizations to receive payment and with other government organizations such as Pay.gov on a need to know basis.

(d) a citation of the legal authority to collect PII and/or BII
USC statutory code 35 U.S.C. Section 2 and 3

(e) the Federal Information Processing Standard (FIPS) 199 security impact category for the system. DBS is a Moderate system.

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.)*

☒ This is an existing information system in which changes do not create new privacy risks. *Continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions	☐	d. Significant Merging	☐	g. New Interagency Uses	☐
b. Anonymous to Non-Anonymous	☐	e. New Public Access	☐	h. Internal Flow or Collection	☐
c. Significant System Management Changes	☐	f. Commercial Sources	☐	i. Alteration in Character of Data	☐
j. Other changes that create new privacy risks (specify):					

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*	☒	e. File/Case ID	☐	i. Credit Card	☒
b. Taxpayer ID	☐	f. Driver's License	☐	j. Financial Account	☒
c. Employer ID	☐	g. Passport	☐	k. Financial Transaction	☒
d. Employee ID	☒	h. Alien Registration	☐	l. Vehicle Identifier	☐
m. Other identifying numbers (specify):					

*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:
Application systems storing their information within a database may capture information related to payroll, user's credentials for access to the application, to process transactions (e.g. customer orders, delivery, etc.), etc.

Social Security numbers are addressed on the front-end systems.

*If SSNs are collected, stored, or processed by the system, please explain if there is a way to avoid such collection in the future and how this could be accomplished:

Social Security numbers are addressed by the front-end systems. For those systems collecting SSNs, their approaches, where applicable, for avoiding collection are identified within those systems' PIAs.

General Personal Data (GPD)					
a. Name	☒	g. Date of Birth	☐	m. Religion	☐
b. Maiden Name	☐	h. Place of Birth	☐	n. Financial Information	☒
c. Alias	☐	i. Home Address	☒	o. Medical Information	☐
d. Gender	☐	j. Telephone Number	☒	p. Military Service	☐
e. Age	☐	k. Email Address	☒	q. Physical Characteristics	☐
f. Race/Ethnicity	☐	l. Education	☐	r. Mother's Maiden Name	☐
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	☐	d. Telephone Number	☒	g. Salary	☐
b. Job Title	☐	e. Email Address	☒	h. Work History	☐
c. Work Address	☒	f. Business Associates	☐		
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	☐	d. Photographs	☐	g. DNA Profiles	☐
b. Palm Prints	☐	e. Scars, Marks, Tattoos	☐	h. Retina/Iris Scans	☐
c. Voice Recording/Signatures	☐	f. Vascular Scan	☐	i. Dental Profile	☐
j. 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	☒	d. 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 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards	☐	Biometrics	☐
Caller-ID	☐	Personal Identity Verification (PIV) Cards	☐
Other (specify):			

☒	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings	☐	Building entry readers	☐
Video surveillance	☐	Electronic purchase transactions	☐
Other (specify):			

☒	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility	☐	For administering human resources programs	☒
For administrative matters	☒	To promote information sharing initiatives	☒
For litigation	☒	For criminal law enforcement activities	☐
For civil enforcement activities	☐	For intelligence activities	☐
To improve Federal services online	☒	For employee or customer satisfaction	☒

For web measurement and customization technologies (single-session)	☒	For web measurement and customization technologies (multi-session)	☒
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

DBS is a general support system for databases at USPTO. It is internally hosted at USPTO. The information maintained in the DBS databases is collected and utilized by USPTO Application Systems.

Databases (DBS) are designed to protect the information while at rest (SC-8) and while in transmission (SC-8) through encryption modules. Encryption is requested by the Application Systems whenever sensitive information will be collected and is implemented case by case. Access restrictions to the applications are enforced by local access through Active Directory Single Sign-On solution.

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 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: • Network and Security Infrastructure System (NSI) • Enterprise Unix Services (EUS) • Enterprise Windows Services (EWS) • Agency Administrative Support System (AASS) • Corporate Administrative Office System (CAOS) • Consolidated Financial System (CFS) • Data Storage Management System (DSMS) • Enterprise Desktop Platform (EDP) • Enterprise Record Management and Data Quality System (ERMDQS) • Enterprise Software Services (ESS) • Enterprise Virtual Events Services (EVES) • Personal Identity Verification System Card Management System (HSPD-12/PIVS/CMS) • Information Dissemination Support System (IDSS) • Intellectual Property Leadership Management System (IPLMSS) • OCIO Program Support System (OCIO-PSS) • PBX-VOIP • Patent Capture and Application Processing System – Examination Support (PCAPS-ES) • Patent Capture and Application Processing System – Capture and Initial Processing (PCAPS-IP) • Patent Search System – Primary Search and Retrieval (PSS-PS) • Patent Search System – Specialized Search and Retrieval (PSS-SS) • Revenue Accounting and Management System (RAM) • Trademark Processing System – External System (TPS-ES) • Trademark Processing System – Internal System (TPS-IS) • Enterprise Monitoring and Security Operations (EMSO) Databases (DBS) are designed to protect the information while at rest (SC-28) and while in transmission (SC-8) through encryption modules. Encryption is requested by the Application Systems whenever sensitive information will be collected and is implemented case by case. Access to the applications is enforced by local access and others through Active Directory Single Sign-On solution.
☐	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 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: DBS is a general support system for databases at USPTO. It is internally hosted at USPTO. The information maintained in the DBS databases is collected and utilized by USPTO Application Systems. These other systems provide this functionality for the data that is being stored. DBS has no authorization to disseminate any type of information since the data stored on DBS is owned by the Application.
☐	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: DBS houses the data that is stored via other information systems within USPTO. These other systems provide this functionality for the data that is being stored. DBS has no authorization to decline any type of information since the data stored on DBS is owned by the Application.

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

☐	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
☒	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: DBS houses the data that is stored via other information systems within USPTO. These other systems provide this functionality for the data that is being stored. DBS has no authorization to decline any type of information since the data stored on DBS is owned by the Application.

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

☐	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how:
☒	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: DBS houses the data that is stored via other information systems within USPTO. These other systems provide this functionality for the data that is being stored. DBS has no authorization to decline any type of information since the data stored on DBS is owned by the Application.

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

☒	All users signed a confidentiality agreement or non-disclosure agreement.
☒	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
☒	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
☒	Access to the PII/BII is restricted to authorized personnel only.
☒	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Access to the PII/BII is being monitored and tracked through audit logs.
☒	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 8/19/2018 ☐ This is a new system.
☒	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 (POAM).
☒	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
☒	Contracts with customers establish ownership rights over data including PII/BII.
☒	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

DBS is a general support system for databases at USPTO. It is internally hosted at USPTO. Databases (DBS) are designed to protect the information while at rest(SC-28) and while in transmission (SC-28) through encryption modules. Encryption is requested by the Application Systems (i.e. front end systems) whenever sensitive information will be collected and is implemented case by case. Access to the applications is enforced by local access and through Active Directory Single Sign-On solution. Information within the databases will be secured consistent with government laws, regulations (e.g. NIST) and USPTO policy.

Section 9: Privacy Act

9.1 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 and number *(list all that apply)*:
☐	Yes, a SORN has been submitted to the Department for approval on (date).
☒	No, a SORN is not being created. The DBS system is not responsible for the information or the records created within the instance. The record creation and retrieval is the responsibility of the application systems collecting the information. This website provides all of the Systems of Records Notices for USPTO: http://www.uspto.gov/web/doc/privacy_sorn.htm.

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: The record control schedule is the responsibility of the system collecting the information. Please refer to the Application PIAs for more details regarding the approved records control schedules.
☐	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 Levels

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.

☐	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 levels. *(Check all that apply.)*

☒	Identifiability	Provide explanation: Required credentials to identify the user (Database User ID and hashed password) when logging on to the database.
☒	Quantity of PII	Provide explanation: PII that might be stored by the Application System. Application PIAs provide detailed information.
☒	Data Field Sensitivity	Provide explanation: PII that might be stored by the Application System. Application PIAs provide detailed information.
☒	Context of Use	Provide explanation: Data that may be used, stored, and transmitted by the Application Systems.
☒	Obligation to Protect Confidentiality	Provide explanation: Sensitive information is encrypted (upon request through CRQ process) whenever an Application notifies DSB that PII will be stored.
☒	Access to and Location of PII	Provide explanation: Data that may be used, stored, and transmitted by the Application Systems.
☐	Other:	Provide explanation:

Section 12: Analysis

12.1 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.

12.2 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.