

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



## Privacy Impact Assessment for the Database Services (DBS)

Reviewed by: John B. Owens II, 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 D. Purvis**

Digitally signed by Katrina D. Purvis  
DN: cn=Catrina D. Purvis, o=Office of the Secretary, Office of Privacy and Open Government, ou=US  
Department of Commerce, email=cpurvis@doc.gov, c=US  
Date: 2017.07.25 13:38:06 -0400

---

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-026-000**

### **Introduction: System Description**

*Provide a description of the system that addresses the following elements:*

*The response must be written in plain language and be as comprehensive as necessary to describe the system.*

*(a) a general description of the information in the system*

The DBS is a general support system for databases at USPTO. It is internally hosted at USPTO's Data Center located at 600 Dulany St, Alexandria, VA 22314. 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.

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 U.S. Treasury/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 122

(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.

<b>Changes That Create New Privacy Risks (CTCNPR)</b>					
a. Conversions	<input type="checkbox"/>	d. Significant Merging	<input type="checkbox"/>	g. New Interagency Uses	<input type="checkbox"/>
b. Anonymous to Non-Anonymous	<input type="checkbox"/>	e. New Public Access	<input type="checkbox"/>	h. Internal Flow or Collection	<input type="checkbox"/>
c. Significant System Management Changes	<input type="checkbox"/>	f. Commercial Sources	<input type="checkbox"/>	i. Alteration in Character of Data	<input type="checkbox"/>
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.)

<b>Identifying Numbers (IN)</b>					
a. Social Security*	<input checked="" type="checkbox"/>	e. File/Case ID	<input type="checkbox"/>	i. Credit Card	<input checked="" type="checkbox"/>
b. Taxpayer ID	<input type="checkbox"/>	f. Driver's License	<input type="checkbox"/>	j. Financial Account	<input checked="" type="checkbox"/>
c. Employer ID	<input type="checkbox"/>	g. Passport	<input type="checkbox"/>	k. Financial Transaction	<input checked="" type="checkbox"/>
d. Employee ID	<input checked="" type="checkbox"/>	h. Alien Registration	<input type="checkbox"/>	l. Vehicle Identifier	<input type="checkbox"/>
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 by the front-end systems, listed in Section 6.2.					
*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, listed in Section 6.2. For those systems collecting SSNs, their approaches, where applicable, for avoiding collection, are identified within those systems' PIAs.

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

<b>Work-Related Data (WRD)</b>					
a. Occupation	<input type="checkbox"/>	d. Telephone Number	<input checked="" type="checkbox"/>	g. Salary	<input type="checkbox"/>
b. Job Title	<input type="checkbox"/>	e. Email Address	<input checked="" type="checkbox"/>	h. Work History	<input type="checkbox"/>
c. Work Address	<input checked="" type="checkbox"/>	f. Business Associates	<input type="checkbox"/>		
i. Other work-related data (specify):					

<b>Distinguishing Features/Biometrics (DFB)</b>					
a. Fingerprints	<input type="checkbox"/>	d. Photographs	<input type="checkbox"/>	g. DNA Profiles	<input type="checkbox"/>
b. Palm Prints	<input type="checkbox"/>	e. Scars, Marks, Tattoos	<input type="checkbox"/>	h. Retina/Iris Scans	<input type="checkbox"/>
c. Voice Recording/Signatures	<input type="checkbox"/>	f. Vascular Scan	<input type="checkbox"/>	i. Dental Profile	<input type="checkbox"/>
j. Other distinguishing features/biometrics (specify):					

<b>System Administration/Audit Data (SAAD)</b>					
a. User ID	<input checked="" type="checkbox"/>	c. Date/Time of Access	<input checked="" type="checkbox"/>	e. ID Files Accessed	<input checked="" type="checkbox"/>
b. IP Address	<input checked="" type="checkbox"/>	d. Queries Run	<input checked="" type="checkbox"/>	f. Contents of Files	<input checked="" type="checkbox"/>
g. Other system administration/audit data (specify):					

<b>Other Information (specify)</b>					

2.2 Indicate sources of the PII/BII in the system. (Check all that apply.)

<b>Directly from Individual about Whom the Information Pertains</b>					
In Person	<input checked="" type="checkbox"/>	Hard Copy: Mail/Fax	<input checked="" type="checkbox"/>	Online	<input checked="" type="checkbox"/>
Telephone	<input checked="" type="checkbox"/>	Email	<input checked="" type="checkbox"/>		
Other (specify):					

Government Sources					
Within the Bureau	<input checked="" type="checkbox"/>	Other DOC Bureaus	<input type="checkbox"/>	Other Federal Agencies	<input type="checkbox"/>
State, Local, Tribal	<input checked="" type="checkbox"/>	Foreign	<input checked="" type="checkbox"/>		
Other (specify):					

Non-government Sources					
Public Organizations	<input checked="" type="checkbox"/>	Private Sector	<input checked="" type="checkbox"/>	Commercial Data Brokers	<input type="checkbox"/>
Third Party Website or Application			<input checked="" type="checkbox"/>		
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	<input type="checkbox"/>	Biometrics	<input type="checkbox"/>
Caller-ID	<input type="checkbox"/>	Personal Identity Verification (PIV) Cards	<input type="checkbox"/>
Other (specify):			

<input checked="" type="checkbox"/>	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	<input type="checkbox"/>	Building entry readers	<input type="checkbox"/>
Video surveillance	<input type="checkbox"/>	Electronic purchase transactions	<input type="checkbox"/>
Other (specify):			

<input checked="" type="checkbox"/>	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	<input type="checkbox"/>	For administering human resources programs	<input checked="" type="checkbox"/>
For administrative matters	<input checked="" type="checkbox"/>	To promote information sharing initiatives	<input checked="" type="checkbox"/>
For litigation	<input checked="" type="checkbox"/>	For criminal law enforcement activities	<input type="checkbox"/>

For civil enforcement activities	<input type="checkbox"/>	For intelligence activities	<input type="checkbox"/>
To improve Federal services online	<input checked="" type="checkbox"/>	For employee or customer satisfaction	<input checked="" type="checkbox"/>
For web measurement and customization technologies (single-session )	<input checked="" type="checkbox"/>	For web measurement and customization technologies (multi-session )	<input checked="" type="checkbox"/>
Other (specify): Financial systems may be collecting the information for payments and generating statements.			

**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 (i.e. front end systems).

Databases (DBS) are designed to protect the information while at rest and while in transmission 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.

**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	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DOC bureaus	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Federal agencies	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
State, local, tribal gov't agencies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Public	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Private sector	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Foreign governments	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Foreign entities	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Other (specify):	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

<input type="checkbox"/>	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.

<input checked="" type="checkbox"/>	<p>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:</p> <p>USPTO Application Systems:</p> <ul style="list-style-type: none"> <li>• Corporate Administrative Office System (CAOS)</li> <li>• Consolidated Financial System (CFS)</li> <li>• Enterprise Software Services (ESS)</li> <li>• Personal Identity Verification System Card Management System (HSPD-12/PIVS/CMS)</li> <li>• Information Dissemination Support System (IDSS)</li> <li>• Intellectual Property Leadership Management System (IPLMSS)</li> <li>• Patent Capture and Application Processing System – Examination Support (PCAPS-ES)</li> <li>• Patent Capture and Application Processing System – Capture and Initial Processing (PCAPS-IP)</li> <li>• Patent Search System – Primary Search and Retrieval (PSS-PS)</li> <li>• Patent Search System – Specialized Search and Retrieval (PSS-SS)</li> <li>• Revenue Accounting and Management System (RAM)</li> <li>• Trademark Processing System – External System (TPS-ES)</li> <li>• Trademark Processing System – Internal System (TPS-IS)</li> </ul> <p>Databases (DBS) are designed to protect the information while at rest and while in transmission 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.</p>
<input type="checkbox"/>	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	<input type="checkbox"/>	Government Employees	<input checked="" type="checkbox"/>
Contractors	<input checked="" type="checkbox"/>		
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.*)

<input type="checkbox"/>	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
<input type="checkbox"/>	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: _____.	
<input checked="" type="checkbox"/>	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 (i.e. front end systems). These front end systems provide this functionality for the data that is being stored. DBS has no authorization to disseminate any type of information since it's owned by the Application.
<input type="checkbox"/>	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

<input type="checkbox"/>	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: DBS houses the data that is stored via USPTO Application Systems (i.e. front end systems). These front end systems provide this functionality for the data that is being stored. DBS has no authorization to decline any type of information since it's owned by the Application.



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

<input type="checkbox"/>	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
<input checked="" type="checkbox"/>	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 USPTO Application Systems (i.e. front end systems). These front end systems provide this functionality for the data that is being stored. DBS has no authorization to decline any type of information since it's owned by the Application.

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

<input type="checkbox"/>	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how:
<input checked="" type="checkbox"/>	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 USPTO Application Systems (i.e. front end systems). These front end systems provide this functionality for the data that is being stored. DBS has no authorization to decline any type of information since it's 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.*)

<input checked="" type="checkbox"/>	All users signed a confidentiality agreement or non-disclosure agreement.
<input checked="" type="checkbox"/>	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
<input checked="" type="checkbox"/>	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
<input checked="" type="checkbox"/>	Access to the PII/BII is restricted to authorized personnel only.
<input checked="" type="checkbox"/>	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.
<input checked="" type="checkbox"/>	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 8/19/2016 <input type="checkbox"/> This is a new system.
<input checked="" type="checkbox"/>	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
<input checked="" type="checkbox"/>	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).
<input checked="" type="checkbox"/>	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
<input checked="" type="checkbox"/>	Contracts with customers establish ownership rights over data including PII/BII.
<input checked="" type="checkbox"/>	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
<input type="checkbox"/>	Other (specify):

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 and while in transmission 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 others 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.”

<input type="checkbox"/>	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number <i>(list all that apply)</i> :
<input type="checkbox"/>	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
<input checked="" type="checkbox"/>	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 is the responsibility of the system collecting the information. The website provided provides all of the Systems of Records Notices for USPTO: <a href="http://www.uspto.gov/web/doc/privacy_sorn.htm">http://www.uspto.gov/web/doc/privacy_sorn.htm</a> .

**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.)*

<input checked="" type="checkbox"/>	There is an approved record control schedule. Provide the name of the record control schedule:
<input checked="" type="checkbox"/>	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.
<input type="checkbox"/>	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:
<input checked="" type="checkbox"/>	Yes, retention is monitored for compliance to the schedule.
<input type="checkbox"/>	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.)*

<b>Disposal</b>			
Shredding	<input checked="" type="checkbox"/>	Overwriting	<input checked="" type="checkbox"/>
Degaussing	<input checked="" type="checkbox"/>	Deleting	<input checked="" type="checkbox"/>
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.

<input type="checkbox"/>	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
<input type="checkbox"/>	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
<input checked="" type="checkbox"/>	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.)

<input checked="" type="checkbox"/>	Identifiability	Provide explanation: Required credentials to identify the user (Database User ID and hashed password) when logging on to the database.
<input checked="" type="checkbox"/>	Quantity of PII	Provide explanation: PII that might be stored by the Application System. Application PIAs provide detailed information.
<input checked="" type="checkbox"/>	Data Field Sensitivity	Provide explanation: PII that might be stored by the Application System. Application PIAs provide detailed information.
<input checked="" type="checkbox"/>	Context of Use	Provide explanation: Data that may be used, stored, and transmitted by the Application Systems.
<input checked="" type="checkbox"/>	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.
<input checked="" type="checkbox"/>	Access to and Location of PII	Provide explanation: Data that may be used, stored, and transmitted by the Application Systems.
<input type="checkbox"/>	Other:	Provide explanation:

## **Section 12: Analysis**

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

<input type="checkbox"/>	Yes, the conduct of this PIA results in required business process changes. Explanation:
<input checked="" type="checkbox"/>	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.

<input type="checkbox"/>	Yes, the conduct of this PIA results in required technology changes. Explanation:
<input checked="" type="checkbox"/>	No, the conduct of this PIA does not result in any required technology changes.