Version Number: 01-2017

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

Privacy Impact Assessment
for the
Reed Technology and Information Services, Inc. (ReedTech®)
Public Data Dissemination (PDD)

Reviewed by: David Chiles, Bureau Chief Privacy Officer (Acting)

☑ 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
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=CATRINA PURVIS, 0.9.2342.19200300.100.1.1=13001002875743
Date: 2018.08.29 11:57:43 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO Reed Technology and Information Services, Inc. (ReedTech®)
Public Data Dissemination (PDD)

Unique Project Identifier: PTOC-025-00

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.
[Guidance: When completing this section, be sure to include only information suitable for public viewing since this is to be posted online. Do not include system information such as IP addresses, architecture diagrams, et.]

(a) a general description of the information in the system
ReedTech PDD is an application information system that is designed to gather and disseminate all publicly available USPTO Patent & Trademark bulk data to the public. The system collects data from various USPTO source systems, packages it into appropriate file containers and delivers it via a public web site. ReedTech hosts the PDD and is required to provide to the public, free of charge, bulk datasets provided by the USPTO and the Public PAIR bulk datasets compiled by ReedTech. A portion of the PDD system is hosted on the FISMA-certified section of the Microsoft Azure system.

(b) a description of a typical transaction conducted on the system
ReedTech provides through the PDD the retrieval and distribution to the public of USPTO patent and trademark bulk data in essentially unaltered form, modified only as necessary to organize or compress the data for ease of distribution or for security purposes. Data dissemination is a continuous system and ReedTech shall continuously monitor the datasets and shall retrieve and host updates and changes as they go forward. ReedTech PDD uses a secure infrastructure, housed external to the USPTO, that performs collection and dissemination of all data to the public at no cost to the public or the USPTO. Such infrastructure may be distributed.

(c) any information sharing conducted by the system
A portion of the PDD system is hosted on the FISMA-certified section of the Microsoft Azure system. The portion of the system residing on Azure hosts the most recent file sets, as they are the most downloaded files, and Azure provides the needed bandwidth to meet the needs of the USPTO's customers.

(d) a citation of the legal authority to collect PII and/or BII
35 U.S.C. 115 and 15 U.S.C. 1501 et seq. The PDD contract requires patents applications to be kept in confidence when required by law (35 U.S.C. 122). Note: any PII or BII is collected by the USPTO and subsequently provided to PDD, but is not collected by PDD itself.

(e) the Federal Information Processing Standard (FIPS) 199 security impact category for the system
*ReedTech PDD is a FIPS 199 **LOW** security impact system.*

Table 1-1 identify the security objective potential impact levels for confidentiality, integrity, and availability. The security impact levels are based on the potential impact definitions for each of the security objectives (i.e., confidentiality, integrity, and availability) discussed in NIST SP 800-60 and FIPS Pub 199.

Table 1-1 Information Type Processed by RTIS PDD and Azure Cloud Enhancement Systems

System Name	Information Type Name	Security Objective			Rationale for Selecting Security Categorization Levels
		Confidentiality	Integrity	Availability	
RTIS PDD	Official Information Dissemination	LOW	LOW	LOW	As NIST recommended.
	Intellectual Property Protection	LOW	LOW	LOW	As NIST recommended.
Azure Cloud Enhancement	Public Relations	LOW	LOW	LOW	NIST recommended.
	General Information	LOW	LOW	LOW	NIST recommended.
	Record Retention	LOW	LOW	LOW	NIST recommended.

Based on the information provided in Table 1-1, Information Types, for RTIS PDD Systems, the high water-mark security impact level for each of the three security objectives of confidentiality, integrity, and availability for RTIS PDD are identified in Table 1-2:

Table 1-2: Security Impact

Security Objective	Security Impact Level
Confidentiality	LOW
Integrity	LOW
Availability	LOW

Table 1-3 identifies security high water-mark categorization for the RTIS PDD's individual subsystems. The baseline set of security controls for each subsystem have been selected and applied in accordance with the high water-mark level for confidentiality, integrity, and availability assigned to that subsystem.

Table 1-3: Security Categorization for RTIS Subsystems

Subsystem Name	Security Categorization
RTIS PDD	LOW

Subsystem Name	Security Categorization
RTIS Azure Cloud Enhancement	LOW

The entire RTIS PDD system has been categorized as having an impact level of Low based on the aggregate high water-mark derived from Table 1-3, as shown in Table 1-4 below.

Table 1-4: **Security Categorization for RTIS PDD**

RTIS PDD Security Categorization	LOW

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: This table does not apply, as no other information is collected by the PDD System NOTE: The PII data contained in the PDD system has already been made public prior to it being added to the					

PDD system. No additional PII data, other than the data that has been made public, is added to or contained within the PDD system.
*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:

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): NOTE: The PII data contained in the PDD system has already been made public prior to it being added to the PDD system. No additional PII data, other than the data that has been made public, is added to or contained within the PDD system.					

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): NOTE: The PII data contained in the PDD system has already been made public prior to it being added to the PDD system. No additional PII data, other than the data that has been made public, is added to or contained within the PDD system.					

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): Not Applicable					

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): Not Applicable. The PDD website requires no authentication and can be accessed completely anonymously.					

Other Information (specify)
This table does not apply, as no other information is collected by the PDD System

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): NOTE: The PII data contained in the PDD system has already been made public prior to it being added to the PDD system. No additional PII data, other than the data that has been made public, is added to or contained within the PDD system.					

Non-government Sources					
Public Organizations	☐	Private Sector	☒	Commercial Data Brokers	☐
Third Party Website or Application			☐		
Other (specify): NOTE: The PII data contained in the PDD system has already been made public prior to it being added to the PDD system. No additional PII data, other than the data that has been made public, is added to or contained within the PDD system.					

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): The PII/BII existing in this system is originally collected to facilitate the processing of patents and trademarks, and to improve Federal services online.			

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).

- Any PII in the PDD system is used solely for the purpose of meeting requirements of the ReedTech PDD / USPTO contract number DOC50PAPT1300006.
- Any PII in the PDD system is submitted by members of the public at the time they submit patent or trademark applications to the USPTO.

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):	☐	☐	☐

*NOTE: The PDD System allows the anonymous public download of granted patent, published patent application, and trademark application files. No authentication is needed, including geolocation of the person performing the download.

☐	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: Microsoft Azure. The purpose of the system is to disseminate patent and trademark data, which includes PII collected by the USPTO.
☐	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): The PII/BII information on the PDD System is accessible to anyone with internet access.			

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: http://www.lexisnexis.com/en-us/terms/privacy-policy.page	
☐	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: Inventors can choose to not submit patent and trademark applications after being instructed that their personal information will be made public as part of the patent and trademark examination process.
☐	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

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: At the time of filing of the patent or trademark application, applicants are notified that patents and trademarks are public information, which includes their PII/BII.
☐	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

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: Throughout the patent lifecycle, Certificates of Correction can be used to update PII/BII data on a patent.
☐	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

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:
☒	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): September 03, 2017 ☐ 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 (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.
☐	Other (specify):

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

• All PDD data is protected through the use of access control permissions, and next generation firewall, anti-virus, and host intrusion detection systems.

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)*: Patent Application Files, COMMERCE/PAT–TM–7 User Access for Web Portals and Information Requests, COMMERCE/DEPT 23
☐	Yes, a SORN has been submitted to the Department for approval on (date).
☐	No, a SORN is not being created.

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:
☒	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: ReedTech is required under the contract to disseminate all available granted patents, published patents applications, and trademark applications. ReedTech is not the office of record for any of this information. This includes any and all patents and trademark data provided by the USPTO to ReedTech for retention during the contract only.
☐	Yes, retention is monitored for compliance to the schedule.
☒	No, retention is not monitored for compliance to the schedule. Provide explanation: ReedTech is required under the contract to disseminate all available granted patents, published patents applications, and trademark applications. ReedTech is not the office of record for any of this information. This includes any and all patents and trademark data provided by the USPTO to ReedTech for retention during the contract only.

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

Disposal			
Shredding	☐	Overwriting	☒
Degaussing	☐	Deleting	☒
Other (specify): Data is deleted or overwritten depending on the point in the information lifecycle that the data is being disposed of.			

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:
☐	Quantity of PII	Provide explanation:
☐	Data Field Sensitivity	Provide explanation:
☒	Context of Use	Provide explanation: The intent of the collection of PII is to allow the patent holder or patent or trademark applicant to be contacted, and for no other purpose.
☐	Obligation to Protect Confidentiality	Provide explanation:
☐	Access to and Location of PII	Provide explanation:
☐	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.