

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



**Privacy Impact Assessment
for the
Reed Tech Patent Data and Document Management (Reed Tech
PDDM)**

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

CHARLES CUTSHALL Digitally signed by CHARLES CUTSHALL
Date: 2025.05.06 11:36:27 -04'00'

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

Date

U.S. Department of Commerce Privacy Impact Assessment USPTO Reed Tech Patent Data and Document Management (Reed Tech PDDM)

Unique Project Identifier: PTOC-065-00

Introduction: System Description

The Reed Tech Patent Data and Document Management (PDDM) system is a FedRAMP approved hybrid system designed to process, transmit and store data and images to support the data-capture and conversion requirements of the United States Patent and Trademark Office (USPTO) patent application process. PDDM is a system owned by LexisNexis Reed Tech sometimes referred to as Reed Tech.

Patent applications are typically submitted to USPTO on paper (hard copy) or in electronic format. Under the PDDM contract, Reed Tech hosts and manages the PDDM system and is required to process the applications, including all text, graphics, artwork, drawings, etc. Once the processing of the applications is completed, each patent is composed and formatted to USPTO specifications for delivery back to USPTO for publication. PDDM process data pertaining to patent application provided to PDDM by the USPTO. Reed Tech has two subcontractors that use PDDM and support Reed Tech's activities as they pertain to processing USPTO information. These subcontractors provide Reed Tech with additional support staff to ensure patents are processed as required within the USPTO – Reed Tech contract. Additionally, PDDM includes video surveillance of the building which house the PDDM system boundary.

Address the following elements:

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

(b) System location

The system is located in Horsham, Pennsylvania, Alexandria VA, and is a Hybrid also being hosted on Microsoft Azure GovCloud FedRAMP. Reed Tech also has two subcontractors, one subcontractor in Palestine, TX and another subcontractor in Roaring Spring, PA. Both handle additional patent processing for the USPTO.

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

PDDM is not a standalone system. There is a USPTO provided site to site Virtual Private Network (VPN) that provides connectivity between jump servers in a DMZ hosted by PDDM and USPTO. PDDM interconnects with the systems below:

- Contractor Access System (CAS):** CAS is an infrastructure information system that provides off-site contractors and selected USPTO employees with limited, monitored, and secured access to USPTO network (PTONet) applications, resources, and services. The CAS network provides contractors with access to the PTONet through the Enterprise Trusted User (ETU) Firewall architecture.

- Network and Security Infrastructure (NSI):** The NSI facilitates the communications, secure access, protective services, and network infrastructure support for all USPTO applications. NSI is PDDM's internal network/security/infrastructure tools that are used to support the USPTO applications. All patents will flow through our NSI tools.

- Patent Capture Application Processing System – Examination Support (PCAPS-ES):** The purpose of PCAPS-ES is to process, transmit and store data and images to support the data-capture and conversion requirements of the USPTO to support the USPTO patent application process.

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

PDDM operates as follows: When patent applications are initially received at the USPTO, the documents are uploaded into the Image File Wrapper (IFW) system which falls under PCAPS-ES. Applications are electronically exported to the PDDM system via a USPTO-managed interconnection.

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

PDDM - Information in the system is retrieved by the user after the patent applications are electronically exported to the PDDM system via a USPTO-managed interconnection.

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

PDDM - Patent applications and application contents are sent to and from the PDDM system via Secured File Transfer Protocol (SFTP).

(g) Any information sharing

Information within PDDM system is shared with internal Reed Tech employees and Reed Tech subcontractors and USPTO employees and USPTO contractors. Reed Tech subcontractors are contractually prohibited from sharing information provided to them as part of the PDDM contract. For all Reed Tech subcontractor's, encrypted information is transferred to them via secure connections.

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

35 U.S.C. 1, 6 and 115, and 5 U.S.C. 301 are the applicable programmatic authorities.

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

Moderate.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

☐ This is a new information system.

☐ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions	<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):					

☐ 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*	<input type="checkbox"/>	f. Driver's License	<input type="checkbox"/>	j. Financial Account	<input checked="" type="checkbox"/>
b. Taxpayer ID	<input type="checkbox"/>	g. Passport	<input type="checkbox"/>	k. Financial Transaction	<input type="checkbox"/>
c. Employer ID	<input type="checkbox"/>	h. Alien Registration	<input type="checkbox"/>	l. Vehicle Identifier	<input type="checkbox"/>
d. Employee ID	<input type="checkbox"/>	i. Credit Card	<input checked="" type="checkbox"/>	m. Medical Record	<input type="checkbox"/>
e. File/Case ID	<input checked="" type="checkbox"/>				
n. Other identifying numbers (specify):					

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

General Personal Data (GPD)

a. Name	<input checked="" type="checkbox"/>	h. Date of Birth	<input type="checkbox"/>	o. Financial Information	<input checked="" type="checkbox"/>
b. Maiden Name	<input type="checkbox"/>	i. Place of Birth	<input type="checkbox"/>	p. Medical Information	<input type="checkbox"/>
c. Alias	<input type="checkbox"/>	j. Home Address	<input checked="" type="checkbox"/>	q. Military Service	<input type="checkbox"/>
d. Gender	<input type="checkbox"/>	k. Telephone Number	<input checked="" type="checkbox"/>	r. Criminal Record	<input type="checkbox"/>
e. Age	<input type="checkbox"/>	l. Email Address	<input checked="" type="checkbox"/>	s. Marital Status	<input type="checkbox"/>
f. Race/Ethnicity	<input type="checkbox"/>	m. Education	<input type="checkbox"/>	t. Mother's Maiden Name	<input type="checkbox"/>
g. Citizenship	<input checked="" type="checkbox"/>	n. Religion	<input type="checkbox"/>		
u. Other general personal data (specify):					

Work-Related Data (WRD)

a. Occupation	<input checked="" type="checkbox"/>	e. Work Email Address	<input checked="" type="checkbox"/>	i. Business Associates	<input type="checkbox"/>
b. Job Title	<input checked="" type="checkbox"/>	f. Salary	<input type="checkbox"/>	j. Proprietary or Business Information	<input checked="" type="checkbox"/>
c. Work Address	<input checked="" type="checkbox"/>	g. Work History	<input type="checkbox"/>	k. Procurement/contracting records	<input type="checkbox"/>
d. Work Telephone Number	<input checked="" type="checkbox"/>	h. Employment Performance Ratings or other Performance Information	<input type="checkbox"/>		
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)

a. Fingerprints	<input type="checkbox"/>	f. Scars, Marks, Tattoos	<input type="checkbox"/>	k. Signatures	<input checked="" type="checkbox"/>
b. Palm Prints	<input type="checkbox"/>	g. Hair Color	<input type="checkbox"/>	l. Vascular Scans	<input type="checkbox"/>
c. Voice/Audio Recording	<input type="checkbox"/>	h. Eye Color	<input type="checkbox"/>	m. DNA Sample or Profile	<input type="checkbox"/>
d. Video Recording	<input type="checkbox"/>	i. Height	<input type="checkbox"/>	n. Retina/Iris Scans	<input type="checkbox"/>
e. Photographs	<input type="checkbox"/>	j. Weight	<input type="checkbox"/>	o. Dental Profile	<input type="checkbox"/>
p. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)

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"/>	f. Queries Run	<input checked="" type="checkbox"/>	f. Contents of Files	<input type="checkbox"/>
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	<input type="checkbox"/>	Hard Copy: Mail/Fax	<input checked="" type="checkbox"/>	Online	<input checked="" type="checkbox"/>
Telephone	<input type="checkbox"/>	Email	<input 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 type="checkbox"/>	Foreign	<input type="checkbox"/>		
Other(specify):					

Non-government Sources					
Public Organizations	<input type="checkbox"/>	Private Sector	<input type="checkbox"/>	Commercial Data Brokers	<input type="checkbox"/>
Third Party Website or Application			<input type="checkbox"/>		
Other(specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

<p>The data in the PDDM system is provided to the USPTO by the Patent applicants. The USPTO provides this information to Reed Tech's PDDM system. Reed Tech employees and Reed Tech subcontractors performs internal quality reviews throughout the lifecycle of the patent process in the PDDM system. USPTO performs inspections of patent deliverables.</p> <p>Patent applicants may update their PII/BII at any time by filing the appropriate forms with the USPTO. The USPTO, in turn, forwards the updated information to Reed Tech's PDDM system as part of standard business processes and the updated PII/BII information would be reflected in the next deliverable to the USPTO.</p>

2.4 Is the information covered by the Paperwork Reduction Act?

<input checked="" type="checkbox"/>	<p>Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.</p> <p>0651-0020, Patent Term Extension 0651-0031, Patent Processing 0651-0032, Initial Patent Applications 0651-0059, Patent Petitions Related to Application and Reexamination Processing Fees 0651-0070, Fee Deficiency Submissions</p>
-------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	0651-0071, Matters Relating to First Inventor to File
<input type="checkbox"/>	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	<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 checked="" type="checkbox"/>	Electronic purchase transactions	<input type="checkbox"/>
Other (specify):			

<input 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			
For a Computer Matching Program	<input type="checkbox"/>	For administering human resources programs	<input type="checkbox"/>
For administrative matters	<input checked="" type="checkbox"/>	To promote information sharing initiatives	<input checked="" type="checkbox"/>
For litigation	<input 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 type="checkbox"/>	For web measurement and customization technologies (multi-session)	<input type="checkbox"/>
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).

PDDM: PII/BII is collected and maintained in this system to facilitate the processing of patent applications for administrative matters, to improve federal online services, to promote information sharing initiatives, and customer satisfaction. The PII/BII comes from persons applying for patents through the USPTO. The video surveillance is used for building security as an extra layer of protection to ensure the integrity of the system.

- 5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

In the event of computer failure, insider threats, or attack against the system by adversarial or foreign entities, any potential PII/BII data PDDM stored within the system could be exposed. In an effort to avoid a breach, PDDM has put certain security controls in place to ensure that 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 and System Auditor and any suspicious indicators such as browsing will be immediately investigated and appropriate action taken.

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. Subcontractors are contractually prohibited from sharing information provided to them as part of the contract with Reed Tech.

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 type="checkbox"/>
DOC bureaus	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Federal agencies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
State, local, tribal gov't agencies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Private sector	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign governments	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign entities	<input type="checkbox"/>	<input 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 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

<input type="checkbox"/>	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
<input type="checkbox"/>	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
<input checked="" type="checkbox"/>	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.

<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>PCAPS-ES CAS</p> <p>NIST security controls are in place to ensure that information is handled, retained, and disposed of appropriately. For example, advanced encryption is used to secure the data both during transmission and while stored at rest. Access to individual's PII is controlled through the application and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. USPTO requires annual security role based training and annual mandatory security awareness procedure training for all employees. All offices of the USPTO adhere to the USPTO Records Management Office's Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citations</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.

6.4 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	<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 checked="" type="checkbox"/>	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
<input checked="" 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: https://www.uspto.gov/privacy-policy	
<input type="checkbox"/>	Yes, notice is provided by other means.	Specify how:
<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: Applicants could only decline to provide PII/BII by declining to continue with the application process. Patent applicants are informed that their PII/BII information will become public as part of the patent process. This notification is provided to the patent applicant by the USPTO upon filing/submission of patent application via the front-end system.

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: Patent applicants do not have the opportunity to consent to particular uses of their PII/BII. They are informed that their PII/BII information will become public as part of the patent process. The applicants must consent to the uses of their PII/BII to go through with the application process via the front-end system.

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: Patent applicants can not directly update their information in Reed Tech PDDM but may update their PII/BII at any time by filing the appropriate forms with the USPTO. The USPTO, in turn, forwards the updated information to Reed Tech as part of standard business processes and the updated PII/BII information would be reflected in the next deliverable to the USPTO.

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. – All PDDM employees sign the agreements and rules of behavior
<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 a authorized personnel only.

<input checked="" type="checkbox"/>	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Reed Tech monitors, tracks, and records access to the PII/BII through an automated logging solution.
<input checked="" type="checkbox"/>	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 5/24/2024 <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
<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 5 recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
<input checked="" type="checkbox"/>	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
<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 type="checkbox"/>	Contracts with customers establish DOC ownership rights over data including PII/BII.
<input type="checkbox"/>	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.- PDDM does not interact with any customers directly. Any impacts to the environment are reported to USPTO and USPTO is responsible for contacting/alerting customers.
<input type="checkbox"/>	Other (specify): The POA&Ms for the system are related to monthly scan compliance and vulnerability testing. 22 POA&Ms were created in Nov, and 14 POA&Ms were created from Nov/Dec scans. The POA&Ms are reviewed often to ensure timely updates and closures.

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.
(Include data encryption in transit and/or at rest, if applicable).

PII within PDDM is secured using appropriate management, operational, and technical safeguards in accordance with NIST requirements. Such management controls include the life cycle review process to ensure that management controls are in place and documented in the System Security Privacy Plan (SSPP). The SSPP specifically addresses the management, operational, and technical controls that are in place and planned during the operation of the system. Operational safeguards include restricting access to PII/BII data to a small subset of PDDM users. All access has role-based restrictions and individuals with access privileges have undergone vetting and suitability screening. Data is maintained in areas accessible only to authorized personnel. PDDM maintains an audit trail and the appropriate personnel is alerted when there is suspicious activity. Data is encrypted in transit and at rest.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g., name or Social Security number)?

- ☒ Yes, the PII/BII is searchable by a personal identifier.
- ☐ No, the PII/BII is not searchable by a personal identifier.

- 9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

<input checked="" type="checkbox"/>	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. <i>(list all that apply):</i> COMMERCE/PAT-TM-7 Patent Application Files covers the patent application records residing in PDDM
<input type="checkbox"/>	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
<input type="checkbox"/>	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.)*

<input checked="" type="checkbox"/>	There is an approved record control schedule. Provide the name of the record control schedule: <ul style="list-style-type: none"> •GRS 5.1, item 020: Non-Recordkeeping Copies of Electronic Records •N1-241-10-1:4.4, Patent Administrative Feeder Records •GRS 6.5, item 010: Customer/Client Records
<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.)*

Disposal			
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 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.)*

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

<input checked="" type="checkbox"/>	Identifiability	Provide explanation: The PDDM system contains PII/BII data that is individually traceable. The combination of name, occupation and other identifiers can easily identify a particular individual.
<input checked="" type="checkbox"/>	Quantity of PII	Provide explanation: These number may vary based on how many applications are received but is in the thousands.
<input checked="" type="checkbox"/>	Data Field Sensitivity	Provide explanation: The PDDM system contains PII/BII data that is individually traceable. The combination of the data in the fields identified in section 2.1 could together make the data fields more sensitive.
<input checked="" type="checkbox"/>	Context of Use	Provide explanation: The PDDM system PII/BII is used as part of the patent application process.
<input checked="" type="checkbox"/>	Obligation to Protect Confidentiality	Provide explanation: Reed Tech and its subcontractors is contractually obligated to protect the confidentiality of the data. This system is governed by The Privacy Act of 1974, which prohibits the disclosure of information from a system of records absents of the written consent of the subject individual unless a statutory exception applies.
<input checked="" type="checkbox"/>	Access to and Location of PII	Provide explanation: The PII/BII data collected by the USPTO is transferred to PDDM system. While the PII/BII is within the PDDM boundary, which is located at secured sites, the data is accessible by individuals not directly employed by the USPTO.
<input type="checkbox"/>	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.)

System users undergo annual mandatory training regarding appropriate handling of information. Physical access to servers is restricted to only a few authorized individuals. The servers storing the potential PII are located in highly sensitive zones within the cloud and logical access is segregated with network firewalls and switches through an Access Control list that limits access to only a few approved and authorized account. USPTO monitors, in real-time, all activities and events within the servers storing the potential PII data and personnel review audit logs received on a regular bases and alert the appropriate personnel when inappropriate or unusual activity is identified.

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

<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.

- 12.3 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.