Version Number: 01-2020

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

Privacy Impact Assessment
for the
Reed Tech Patent Data Capture (PDCap)

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

Jennifer Goode 02/25/2021

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO Reed Tech PDCap

Unique Project Identifier: PTOC-013-00

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.

The Reed Tech Patent Data Capture (PDCap) system is designed to process, transmit and store data and images to support the data-capture and conversion requirements of the USPTO patent application process. Patent applications are typically submitted to USPTO on paper (hard copy) or in electronic format. Under the Patent Data Capture contract, Reed Tech hosts and manages the PDCap system and is required to convert the paper applications into an electronic format, including all text, graphics, artwork, drawings, etc. Once converted to electronic data, each patent is composed and formatted to USPTO specifications for delivery back to USPTO. The

Reed Tech Published Application Alert Service (PAAS) is a service offered by the USPTO to allow the public to configure queries and alerts for key words in pre-grant published patent applications.

(a) Whether it is a general support system, major application, or other type of system
Reed Tech PDCap is a major application and a contractor system.

(b) System location
Primary location: 7 Walnut Grove Drive, Horsham, PA 19044
Secondary location: 2331 Mill Road, Suite 300, Alexandria, VA 22314

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
It is not a standalone system. A point-to-point DS3 provides connectivity between the Horsham, PA, location and the Alexandria, VA, location. A point-to-point DS3 is a wide area network (WAN) connection to USPTO. This connection is owned and managed by USPTO, as is the equipment hosting the connection. It is an extension of the IFW network. There is a fail-over VPN connection between the two sites that provides fault tolerance for the point-to-point connection. Additionally Reed Tech has subcontractors supporting PDCap and transfers USPTO data to the subcontractor locations. Traffic permitted into the network from the internet includes the following traffic to servers in the De-Militarized Zone (DMZ):

- Encrypted FTP traffic to public FTP server

- Remote access VPN
- Public email
- Backup point-to-point VPN (Internet Protocol Security [IPSEC]) for
- Alexandria location (only used when primary link fails).

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

- The Reed Tech Patent Data Capture (PDCap) system is designed 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.
- The Reed Tech Published Application Alert Service (PAAS) is a service offered by the USPTO to allow the public to configure queries and alerts for key words in pre-grant published patent applications.

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

- PDCap - Information in the system is retrieved by the user after the patent applications are electronically exported to the Reed Tech PDCap system via a USPTO-managed- interconnection. Every application is then examined by a Reed Tech proprietary application which breaks down each page into separate sections, such as graphics and text. Each section is then sent to separate directories on the Reed Tech PDCap network for manipulation by the different departments dedicated to text, headers, and complex work units such as math, chemistry, and drawings.
- PAAS – Information in the system is retrieved by the user after a logged-in user creates a keyword search, which will be executed on a weekly basis against only the most recent pre-grant published patent application.

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

Patent applications are sent to and from the PDCap system via Secured File Transfer Protocol (SFTP).

(g) Any information sharing conducted by the system

Information sharing occurs with members of the public via PAAS; where members of the public can retrieve information via a keyword search. Additionally, information sharing occurs with subcontractors. Subcontractors are contractually prohibited from sharing information provided to them as part of the PDCap contract. For all subcontractors, 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. 2 and 115. Refer to Reed Tech PDCap contract DOC50PAPT1500003 for requirements to collect minimum data necessary to provide contracted services.

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

☐ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

☒ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or 01-2017).

☐ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2019 or later).

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*	☐	f. Driver's License	☐	j. Financial Account	☐
b. Taxpayer ID	☐	g. Passport	☐	k. Financial Transaction	☐
c. Employer ID	☐	h. Alien Registration	☐	l. Vehicle Identifier	☐
d. Employee ID	☐	i. Credit Card	☐	m. Medical Record	☐
e. File/Case ID	☐				
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	☒	h. Date of Birth	☐	o. Financial Information	☐
b. Maiden Name	☐	i. Place of Birth	☐	p. Medical Information	☐
c. Alias	☐	j. Home Address	☒	q. Military Service	☐

d. Gender	☐	k. Telephone Number	☐	r. Criminal Record	☐
e. Age	☐	l. Email Address	☒	s. Physical Characteristics	☐
f. Race/Ethnicity	☐	m. Education	☒	t. Mother's Maiden Name	☐
g. Citizenship	☐	n. Religion	☐		
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	☒	e. Work Email Address	☒	i. Business Associates	☐
b. Job Title	☒	f. Salary	☐	j. Proprietary or Business Information	☒
c. Work Address	☒	g. Work History	☐	k. Procurement/contracting records	☐
d. Work Telephone Number	☒	h. Employment Performance Ratings or other Performance Information	☐		
l. Other work-related data (specify):					

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

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): log on/log off; success/failure					

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

The data in the PDCap system is provided by the Patent applicants, and is provided to Reed Tech by the USPTO. Reed Tech performs internal quality reviews throughout the lifecycle of the patent process. USPTO performs inspections of patent deliverables. For the PAAS system the data is provided by users, who register at the website with a valid email address.

2.4 Is the information covered by the Paperwork Reduction Act?

☒	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. 0651-0032 Initial Patent Applications, 0651-0031 Patent Processing
☐	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

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

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

Section 3: System Supported Activities

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

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

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

Section 4: Purpose of the System

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

Purpose			
For a Computer Matching Program	☐	For administering human resources programs	☐
For administrative matters	☐	To promote information sharing initiatives	☒
For litigation	☐	For criminal law enforcement activities	☐
For civil enforcement activities	☐	For intelligence activities	☐
To improve Federal services online	☒	For employee or customer satisfaction	☐
For web measurement and customization technologies (single-session)	☐	For web measurement and customization technologies (multi-session)	☐
Other (specify): PII/BII is gathered and provided to RTIS by the USPTO as part of the Patent application process. Patents issued in the name of applicant, Assignee listed on patent, other requirements, and etcetera. Additionally, the following items were checked because they apply to PAAS: 'To improve Federal services online' and 'To promote information sharing initiatives'.			

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).

• PDCap: PII/BII is collected and maintained in this system to facilitate the processing of patents and trademarks. The PII/BII comes from members of the public applying for patents through the USPTO.
• PAAS: This PII/BII information is used solely to generate patent alerts, which is the purpose of the PAAS. Members of the public may create user profiles in the PDCap Published Application Alert Service (PAAS). These user profiles contain the full name and email address of the person creating the profile. The full name is used only for password reset instances.

5.2 Describe any potential threats to privacy 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 accordance with the USPTO Information Security guidelines, the PDCap system is designed and administered to ensure the confidentiality of PII provided to Reed Tech by the USPTO.

Insider threat is a potential threat to privacy. To mitigate insider threat, Reed Tech has included insider threat awareness training as part of their Annual Security Awareness Training requirement.

Specific safeguards that are employed by the PDCap system to protect the patent applications and the PII data contained include:
• The PDCap system and its facility are physically secured and closely monitored. Only individuals authorized by Reed Tech to access USPTO data are granted logical access to the system.
• All patent information is encrypted when transferred between Reed Tech and USPTO and between our subcontractors using secure electronic methods.
• Technical, operational, and management security controls, as defined in NIST SP 800-53, Rev. 4, for a Moderate risk system, the USPTO Information Security Handbook, and other guidelines, are in place at Reed Tech and are verified regularly.
• Periodic security testing is conducted on the PDCap system to help assure that any new security vulnerabilities are discovered and fixed.

• All PDCap personnel are trained to securely handle patent information and to understand their responsibilities for protecting patents. Reed Tech conducts annual IT Security Awareness Training for all PDCap personnel and all new hires. This training includes, but is not limited to, the following topics: insider threat, social engineering, phishing, telework and travel, PII, BII, safeguarding sensitive information, best practices for mobile devices, password protection, cybersecurity incidents, incident response, and rules of the road. Regarding the PAAS system, threats to privacy are limited as RTIS only collects first name, last name and email address. However, Reed Tech has a full complement of controls in place to protect the PII data that is collected as part of the system, similar to the controls in place for the PDCap system.

Access to the PAAS data is limited to only those with business needs to access it and the PAAS system, as part of the PDCap system, is subject to annual assessment of the in-place controls.

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 USPTO provides Reed Tech with a copy of the patent application data, and retains a copy within their systems. Reed Tech shares PII/BII data only with PDCap subcontractors	☐	☒	☐

☐	The PII/BII in the system will not be shared.

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

☒	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re- dissemination of PII/BII.
☐	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
☐	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

☒	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: • PDCap: The PDCap system connects with USPTO NSI to exchange patent information (including

	PII/BII), which is provided from USPTO to Reed Tech initially. This information exchange is done over secure connections between the PDCap facilities and the USPTO facility. The descriptions of the technical controls protecting the information exchange are listed in the PDCap System Security Plan (SSP). These controls include, but are not limited to, encryption, authentication, access controls, etc. • PAAS: The PAAS system does not connect with or receive information, including PII/BII, from any other IT systems.
☐	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public	☒	Government Employees	☒
Contractors	☒		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

☒	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
☒	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://www.uspatentappalerts.com.	
☐	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: PDCap: Patent applicants are informed that their PII/BII information will become public as part of the patent process. The applicants have the opportunity to not submit their patent application if they decline to provide PII/BII data. This notification is provided to the patent applicant by the USPTO upon filing/submission of patent application. Reed Tech protects the collected information by implementing all controls in NIST SP 800-53, Rev. 4, and obtains Authority to Operate (ATO) from the USPTO.

		PAAS: All users must read the terms and conditions and click to agree to them prior to registering to use the PAAS system. Not doing so constitutes opting out and declining to provide PII/BII.
☐	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: PDCap: Patent applicants consent to the use of their PII/BII for the purposes of processing the patent application. There are no uses of the PII/BII beyond the processing of the patent application. This notification is provided to the patent applicant by the USPTO upon filing/submission of patent application. Reed Tech protects the collected information by implementing all controls in NIST SP 800-53, Rev. 4, and obtains Authority to Operate (ATO) from the USPTO. PAAS: All users must read the terms and conditions and click to agree to them prior to registering to use the PAAS system. There are no uses of the PII/BII beyond basic system function.
☐	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: PDCap: 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 as part of standard business processes and the updated PII/BII information would be reflected in the next deliverable to the USPTO. PAAS: The PAAS terms of use state that individuals have the opportunity to review/update PII/BII pertaining to them. The PII/BII data is available to be reviewed/updated at any time on the user's profile page.
☐	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: Applicable to PDCap and PAAS: Reed Tech monitors, tracks and records access to the PII/BII through an automated logging solution.
☒	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): April 29, 2020 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
☒	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
☒	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
☒	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.
☒	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
☐	Contracts with customers establish 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.
(Include data encryption in transit and/or at rest, if applicable).

PDCap: The PDCap system is protected through multiple layers of security controls. All hosts on the PDCap system are hardened according to CIS secure benchmarks. The system is also protected with next-generation firewalls, antivirus, intrusion detection systems, and spam filtering. The PDCap system employs FIPS 140-2 compliant and validated cryptographic mechanisms to ensure data encryption.

PAAS: The PAAS database is hardened according to CIS secure benchmarks. Access to the PAAS database is limited per user and host. The database is on a dedicated subnet, and is not accessible from the Internet. Passwords must meet complexity requirements and are encrypted. The login and registration pages are delivered over HTTPS. There is an automatic account lockout period after a defined period of inactivity.

- The PDCap and PAAS system and its facility are physically secured and closely monitored. Only individuals authorized by PDCap and PAAS to access USPTO data are granted logical access to the system.

- All patent information is encrypted when transferred between PDCap and USPTO and PAAS using secure electronic methods.
- Technical, operational, and management security controls are in place at PDCap and PAAS and are verified regularly.
- Quarterly security scans are conducted on the PDCap and PAAS system to help assure that any new security vulnerabilities are discovered and fixed.
- All PDCap and PAAS personnel are trained to securely handle patent information and to understand their responsibilities for protecting patents.

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."

☒	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: • COMMERCE/PAT-TM-7 Patent Application Files covers the patent application records residing in PDCap. • COMMERCE/PAT-TM-23 User Access for Web Portals and Information Requests covers the records residing in PAAS.
☐	Yes, a SORN has been submitted to the Department for approval on (date).
☐	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

☒	There is an approved record control schedule. Provide the name of the record control schedule: 1) N1-241-10-1:4.2, Patent Examination Working Files – (1a) The tapes temporarily house the data, prior to export, and are considered "working files" 2) N1-241-10-1:4.4, Patent Examination Feeder Records – (2a) When 'fed' into the system, these

	feeder documents become records 3) GRS 5.1:020, Non-recordkeeping copies of electronic records – (3a) The tapes which held the feeder data, now become non-records
☐	This is not required per the contract. Once Reed Tech completes work on USPTO files and the final deliverables are returned to the USPTO, the completed data is also archived by Reed Tech to encrypted tapes that are stored in the Reed Tech data center.
☒	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. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

☐	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
☒	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
☐	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

☒	Identifiability	Provide explanation: The non-sensitive data given including Name, Home Address, Email Address and User Id could be used to identify an individual. Because social security numbers are not collected, maintained, or disseminated, the PII is considered to be non-sensitive.
☐	Quantity of PII	Provide explanation:

☒	Data Field Sensitivity	Provide explanation: Combination of name, home address and telephone number may allow the data to be more identifiable. Because social security numbers are not collected, maintained, or disseminated, the PII is considered to be non-sensitive.
☐	Context of Use	Provide explanation:
☒	Obligation to Protect Confidentiality	Provide explanation: Reed Tech is contractually obligated to protect the confidentiality of the data.
☒	Access to and Location of PII	Provide explanation: • PDCap: The PII/BII data collected by the USPTO is transferred to Reed Tech. While it is at Reed Tech, that data is accessible by individuals not directly employed by the USPTO. • PAAS: The PAAS system contains PII that is individually traceable. For the PAAS system RTIS only collects first name, last name, and email address. The full name is only used for password reset instances.
☐	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.)

For the PDCap system, the patent applicants acknowledge and also get notified that their information will become public at the time of filing the patent application. Insider threat is a potential threat to privacy. To mitigate insider threat, Reed Tech has included insider threat awareness training as part of their Annual Security Awareness Training requirement.

For the PAAS system, threats to privacy are limited as RTIS only collects first name, last name, and email address. RTIS collects the minimum amount of data required to fulfill the terms of the contract.

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

☐	Yes, the conduct of this PIA results in required business process changes. Explanation:

☒	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

☐	Yes, the conduct of this PIA results in required technology changes. Explanation:
☒	No, the conduct of this PIA does not result in any required technology changes.