Template Version Number: 01-2020

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

Privacy Impact Assessment
for the
Patent Trial and Appeal Case Tracking System (P-TACTS)

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 12/07/2021

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO Patent Trial and Appeal Case Tracking System (P-TACTS)

Unique Project Identifier: PTOP-010-00

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 Patent Trial and Appeal Board reviews appeals by patent applicants who disagree with a decision by a Patent Examiners on their pending patent applications. We handle 6,000 to 8,000 a year. The Board typically also conducts less than one thousand post-grant Patent proceedings a year in which two parties contest whether the Patent Office should have issued the patent. Most post-grant patent proceedings are filed under the Leahy-Smith American Invents Act (AIA). By far most of the entities involved in post-grant proceedings are organizations. In rare post-grant proceedings, an individual is a petitioner or patent owner. As required by 37 C.F.R. § 42.8, petitioners and patent owners must file a notice identifying real party-in-interest, lead and back-up counsel (if party is represented by counsel), and applicable service information (electronic mail address, postal mailing address, a hand-delivery address if different than the postal address, a telephone number, and a facsimile number). Counsel information includes attorney name, email, USPTO Registration Number, phone number, and fax number.
Patent Trial and Appeal Case Tracking System (P-TACTS) supports the Board in managing these cases.

For the appeals the Board decides, the documents for the patent applications and appeals are stored in other patent systems, not in P-TACTS. P-TACTS stores status information about cases in a database, which is used by internal PTAB users and is not accessible to the public.
For post-grant patent proceedings, P-TACTS stores the case documents. Some of those documents are filed by the parties to the proceedings, so there is an external portal for doing so and viewing case documents. To file documents, external users need to establish a user account. A public user is required to provide first name, last name, a phone number, and an email address. Board decision public documents are available for post-grant patent proceedings and appeals from the USPTO's Big Data Repository/API system, which is not part of P-TACTS and is not managed by the Board. Public users, however, also can use P-TACTS to search proceedings by the review number assigned to each post-grant patent proceedings, party name, etc. A public user is required to provide first name, last name, a phone number, and an email address.

(a) Whether it is a general support system, major application, or other type of system
P-TACTS is a Major Application.

(b) System location
600 Dulany Street, 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)

P-TACTS interconnects with other systems including the following Major Applications:

1. **Enterprise Software Services (ESS)** is a collection of applications that centralizes common business applications and tools for modeling how the agency functions, assists with unique application development, improves business logic and support, and improves communications and collaboration within the agency.

2. **Patent Capture and Application Processing System – Internal Support (PCAPS-IP)** is a master system that is comprised of multiple Automated Information Systems that perform specific functions, which includes patent submissions, patent categorization, metadata capture, and patent examiner assignment of patent applications. PCAPS-IP users include both internal USPTO personnel as well as the public.

3. **Patent Capture and Application Processing System – Examination Support (PCAPS-ES)** is a master system that enables patent examiners and public users to search and retrieve application data, images, and patent applicants in order to identify individuals and organizations with intellectual property, pre-grant, and published applications.

4. **Patents End-to-End (PE2E)** is a master system portfolio consisting of next generation Patent Automated Information Systems (AISs) with a goal of creating a single web-based examination tool, which provides users with unified and robust interface that does not require launching of separate applications in separate windows.

5. **Intellectual Property Leadership Management Support Systems (IPLMSS)** is a master AIS which facilitates grouping and managing of 10 general support and separately bounded AISs that collectively support the USPTO Director, Deputy Director, Office of the General Counsel (OGC), including OGC's components the Office of General Law (OGL), Office of the Solicitor, and Office of Enrollment and Discipline (OED), Trademark Trial and Appeal Board (TTAB), Patent Trail and Appeal Board (PTAB), Office of Patent Training (OPT), and Office of Policy and International Affairs (OPIA).

6. **Fee Processing Next Generation (FPNG)** is a master system that provides payment method to the public and internal facing functionality that enables USPTO employees to support customers.

7. **Agency Administrative Support System (AASS)** is a master system that supports multiple enterprise administrative functions. AASS enables the Under Secretary of Commerce for Intellectual Property and Director of the USPTO to receive and respond to

a wide range of official correspondence by electronically capturing, routing and tracking both incoming and responding documents. As an automated document management system, AASS supports the Office of Policy and International Affairs (OPIA) with the capabilities of capturing, indexing, searching and retrieving documents. AASS provides the Chief Economist's office with a solution to store data and perform statistical analysis in a secured environment.

8. **Information Delivery Product (IDP)** is a master system that provides access to integrate USPTO data through various tools in support of not only reporting and visualizing but also analytics used in decision-making across USPTO.

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

P-TACTS is a Major Application for supporting USPTO's administrative law body Patent Trial and Appeal Board (PTAB) for electronically filing documents in connection with Inter Partes Review (IPR), Covered Business Method Patents (CBM), Post Grant Review (PGR), and Derivation Proceedings (DER), established under the Leahy-Smith America Invents Act (AIA). It is also used for the administrative processing of pre-Grant Appeals of certain types of adverse decisions by patent examiners. Appeals documents are stored in P-ELP (Patents content management system) and the statuses are recorded for the cases in the Appeals database. The addresses of the Appellants are stored in PALM and the Appeals database does not store the address. P-TACTS also updates PALM on transaction codes. The Appeals database records only the transactions pertaining to the Appeal processing by the P-TACTS. This database is only used for Appeal processing by internal P-TACTS users; it is not used or accessible to the public. In addition, P-TACTS provides case management, case tracking and notification, hearing schedule, data analytics and reporting capabilities, data search and search results, data integration, data synchronization, and data store, document submission and management, workload balance and management and electronic records management.

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

As internal users, P-TACTS administrators have access to the new queue of petitions for assignment. They are able to see certain attributes of the available judges so they can properly and accurately assign petitions to the appropriate judge. There are two types of hearing teams, one team has access to papers related to appeals and use a case number to search the system, the other team can search AIA cases by entering a case number to search the system similar to how the judges will access the system.

As internal users, supervisory paralegals and some paralegals have access to the Import Manager screens to automatically import appeal cases into P-TACTS. They also have access to the Post Decisional Case Management screen to view recently decided cases.

As internal users, Judges have access to all the available petitions that they are assigned to or are given permission to access. In addition, judges and patent attorneys, have case dockets that they can view with all the cases that are assigned (paralegals do not). All internal users have assignment dockets for tasks they are assigned.

Public (External) users can review/search the P-TACTS documents/filings/proceedings without logging into the system. Public users can search by 'AIA Review Number, Patent Number, Application Number, Party Name, AIA Review/Case Type, and Tech Center.' Public users have read only access to the documents. Public users create their own account from the P-TACTS website by clicking on 'Create an Account' for the following actions:

> *Person or group who challenges the validity of the AIA proceedings; Person or group who has or claims to have the ownership of the AIA proceeding; Patent application or Owner who is appealing a final office decision; Applicants or Patent Owners involved in challenge over inventor ship; Persons or groups other than the Patent Owner/Appellant or the public, who actively participates in the validity of challenges of proceeding.*

A public user is required to provide First name, Last Name, Phone Number, and Email Address. Additionally, the public user is also required to create a password in the Register a New Account form. After the user clicks on "register" an email is sent out by the system to the user with instructions and a link to validate/activate the account. When the user clicks on the provided link, a screen with validation code is displayed, user clicks on submit, account is activated and a message "You've successfully registered for PTAB E2E!" is displayed.

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

P-TACTS implements cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission. For external facing systems, HTTPS and TLS 1.2 or high, AES with 256-bit encryption, RSA with 2048-bit exchange as key exchange mechanisms are used. However, for SSL usage, all activities are internal to USPTO and per OMB M-15-13, internal use of HTTPS is encouraged but not required.

(g) Any information sharing conducted by the system

Yes. P-TACTS implements the Board's post-grant patent proceedings rules, which aim to strike a balance between the public's interest in maintaining a complete and understandable file history and the parties' interest in protecting truly sensitive information. 77 Fed. Reg. 48761 (Section E. Public Availability and Confidentiality). The system allows parties to file information with a motion to seal and to mark the information as viewable to "Board and Parties Only." The information is provisionally sealed pending outcome of the decision on the motion. That information is not shared with the public unless the Board denies the motion to seal. 77 Fed. Reg. 48761 (Section E. Public Availability and Confidentiality).

The name of the judges on the panel issuing a Board decision or order are included in the decision or order. For post-grant patent proceedings, counsel name, employer, and email address of counsel representing petitioners and patent owners is included at the end of each Board decision or order. User account information is not shared.

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

5 U.S.C. 301, 44 U.S.C. 3101, 35 U.S.C. 134, 135, 311-318, and 321-328.

(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	☒	f. Queries Run	☒	f. Contents of Files	☐
g. Other system administration/audit data (specify):					

Other Information (specify)

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

Directly from Individual about Whom the Information Pertains					
In Person	☐	Hard Copy: Mail/Fax	☐	Online	☒
Telephone	☐	Email	☐		
Other (specify):					

Government Sources					
Within the Bureau	☐	Other DOC Bureaus	☐	Other Federal Agencies	☐
State, Local, Tribal	☐	Foreign	☐		
Other (specify):					

Non-government Sources					
Public Organizations	☐	Private Sector	☒	Commercial Data Brokers	☐
Third Party Website or Application			☐		
Other (specify):					

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

Non-privileged users of P-TACTS are prevented from executing privileged functions by the concept of least privilege. Only administrators have access to privileged functions. Access to privileged functions is approved by the Technical Lead or business unit before assigning to administrators. Additionally, integrity verification to detect unauthorized changes to include Windows log transfer configuration, Unix sys log parameters, NTP values, SNMP values, local admin accounts, user groups, and client parameters monitoring are done at Enterprise Unix Services (EUS), Enterprise Windows Services (EWS), and Security Compliance Services (SCS) interconnected systems levels.

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. 0651-0063 PTAB Actions 0651-0069 Patent Review and Derivations
☐	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 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	☐	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): For correspondence (by email) purposes and to review the progress of petitions and to run internal reports to be used by USPTO business unit.			

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).

The system administration/audit data (SAAD) in Section 2.1 is collected from members of the public who access P-TACTS for post-grant patent proceedings. The SAAD information in Section 2.1 is collected from DOC employees and contractors who access P-TACTS. P-TACTS enables the public (registered or anonymous) to search for AIA reviews by the party name, AIA Review/Case type, patent number or application number, PTAB proceedings and documents related to proceedings. P-TACTS also provides this public data as bulk downloads. P-TACTS collects, maintains and disseminates data that may contain the following types of public PII (U.S. and foreign):

Patent applicant PII (i.e., applicant's name, correspondence address, email, telephone number etc.) which is of a public nature to facilitate the patent application process or correspondence between the patent applicant and USPTO.

Federal employee PII (i.e. employee name, email, telephone number and USPTO official mailing address etc.) which is used externally for correspondence to the patent applicant(s) and internally for USPTO business unit's reports.

PTAB business units conducts post-grant petition Trials and pre-grant appeals. They include inter Partes disputes, covered business method patent reviews and derivation proceedings; hearing appeals from adverse examiner decisions in patent applications and reexamination proceedings; and rendering decisions in interferences. Public PII may be contained within these internal business processes.
P-TACTS does access BII (i.e. unpublished patent applications) stored on Patent Capture and Application System – Examination Support (which is approved for PII/BII); however, P-TACTS does not store, collect or disseminate BII in these types of cases.

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.)

Potential threats to privacy include insider threats, adversarial entities and foreign governments. Unauthorized access and unauthorized changes to information are also threats to the system. P-TACTS handles and retains both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. Only people authorized to access the system are allowed to handle the information or access the information retained within the system. P-TACTS also uses access control mechanisms implemented on all of its components to ensure the information is handled and retained in accordance with all applicable laws and requirements. System records are retained in accordance with National Archives and Records Administration approved records control schedules. P-TACTS is used to support determinations in inter-parties disputes. Only limited internal P-TACTS users have access to an assigned dashboard and their work queue and are able to view petitions. Judges have access to petitions that they are assigned to or have been given permission to access.

USPTO employees and contractors receive mandatory training regarding appropriate handling of information; employees and contractors received training on privacy and confidentiality policies and practices, or system users undergo annual mandatory training regarding appropriate handling of information.

Until petitions are final, petitions are accessible only to limited internal users. After petitions are final, these become public documents. Printing is done by authorized users only; printed documents are picked up as soon as documents are printed. Information is not disposed of except in accordance with applicable record control schedules. Additionally, the system owner is responsible for ensuring that the P-TACTS is deployed and operated in accordance with the agreed-upon security controls, that the support personnel receive requisite security training, and that necessary resources are available for the Security Authorization processes.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	☐	☐	☒
DOC bureaus	☐	☐	☐
Federal agencies	☐	☐	☐
State, local, tribal gov't agencies	☐	☐	☐
Public	☒	☒	☒
Private sector	☐	☐	☐
Foreign governments	☐	☐	☐
Foreign entities	☐	☐	☐
Other (specify):	☐	☐	☐

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

6.2 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: P-TACTS interconnects with other systems including the following Major Applications: • Enterprise Software Services (ESS) • Patent Capture and Application Processing System – Internal Support (PCAPS-IP) • Patent Capture and Application Processing System – Examination Support (PCAPS-ES) • Patents End-to-End (PE2E) • Intellectual Property Leadership Management Support Systems (IPLMSS) • Fee Processing Next Generation (FPNG) • Agency Administrative Support System (AASS) • Information Delivery Product (IDP) P-TACTS also uses access control mechanisms implemented on all of its components to ensure the information is handled and retained in accordance with all applicable laws and requirements. The technical access controls are securely managed through Active Directory and Enterprise Unix permission enforcements. Although PTAB interconnects with other USPTO master systems authorized to process PII/BII, PTAB does not retrieve any sensitive PII/BII from those systems. There are infrastructure and other OCIO established technical controls and administrative policies, which include password authentication at the server and database levels. HTTPS/TLS is used for all data transmissions to and from the Internet, USPTO DMZ, and PTOnet. A dedicated socket is used to perform encryption and decryption and where appropriate data at rest encryption is leveraged.
☐	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: http://www.uspto.gov/privacy-policy.	
☐	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: Individuals have an opportunity to decline to provide their PII/BII but without providing name, email address, address and telephone number, petition cannot be filed, submitted and reviewed adequately.
☐	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: Individuals sign their applications for petition during submission and this authorizes the use of their PII/BII. Individuals volunteer to provide their name, email, correspondence address, phone number etc. in order to file petitions for review.
☐	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: Users can login to their accounts and update their information.
☐	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: system monitoring is enabled by default to send system and security logs to the OCIO Command Center (C3), who review and analyze system logs for inappropriate or unusual activities.
☒	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): _1/29/21_____ ☐ 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 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 DOC 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).*

In accordance with NIST 800-18 Rev. 1 and NIST 800-53 Rev. 4, the P-TACTS System Security Plan (SSP) addresses the extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment. The SSP is reviewed on an annual basis. In addition, annual assessments and Continuous Monitoring reviews are conducted on the P-TACTS data. The USPTO Office of Policy and Governance/Cybersecurity Division (OPG/CD) conducts these assessments and reviews based on NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations and NIST SP 800-53A Revision 4 Assessing Security and Privacy Controls in Federal Information Systems and Organizations. The results of these assessments and reviews are documented in the P-TACTS Security Assessment Package as part of the system's Security Authorization process.

Management Controls

USPTO uses the Life Cycle review process to ensure that management controls are in place for P-TACTS. During the enhancement of any component, the security controls are reviewed, re-evaluated, and updated in the System Security Plan. The System Security Plan specifically addresses the management, operational, and technical controls that are in place, and planned, during the operation of the enhanced system. Additional management controls include performing national agency checks on all personnel, including contractor staff.

Additionally, USPTO develops privacy and PII-related policies and procedures to ensure safe handling, storing, and processing of sensitive data.

Operational Controls

Automated operational controls include securing all hardware associated with the P-TACTS in the USPTO Data center. The Data Center is controlled by access card entry and is manned by a uniformed guard service to restrict access to the servers, their Operating Systems and databases.

Technical Controls

P-TACTS is secured by various USPTO infrastructure components, including the Network and Security Infrastructure (NSI) system and other OCIO established technical controls to include password authentication at the server and database levels. Web communications leverages modern encryption technology such as TLS over HTTPS. Dedicated interconnections offer protection through IPSec VPN tunnels. P-TACTS PII/BII is encrypted.

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, number, and link. *(list all that apply)*: Parties Involved in Patent Interference Proceedings PAT/TM-6 Litigation, Claims, and Administrative Proceeding Records—COMMERCE/DEPT-14 Attorneys and Agents Registered or Recognized to Practice Before the Office –PAT/TM-1 Users of Public Facilities of the Patent and Trademark Office –PAT/TM-14 Patent Application Files—PAT/TM-7
☐	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: N1241-10-1:7.4 Patent Legal Correspondence N1-241-09-1:b2.1 Patent Interference Cases – Open to the Public N1-241-09-1:b2.3 Patent Appeal Cases N1-241-09-1:b2.6 Patent Appeal and Interference Case Tracking
☐	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
☒	Yes, retention is monitored for compliance to the schedule.
☐	No, retention is not monitored for compliance to the schedule. Provide explanation:

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

Disposal			
Shredding	☐	Overwriting	☐
Degaussing	☐	Deleting	☒
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact 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.)*

☒	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 level. *(Check all that apply.)*

☒	Identifiability	Provide explanation: P-TACTS collects, maintains, or disseminates PII about public users such as name, home/business address, email address, and telephone number etc. When combined this data directly identified individuals. If PII were inappropriately accessed, used, or disclosed potential harm could result to the subject individuals and or the organization.
☒	Quantity of PII	Provide explanation: There are an estimated ~200k records

		comprised of ~50k petitions and affiliated attorney actions. Since attorneys are involved in multiple cases, the actual number of records with unique PII will be less than ~200k.
☒	Data Field Sensitivity	Provide explanation: This data includes limited personal and work related elements for identifying and authenticating user and the combination does not make the data fields more sensitive.
☒	Context of Use	Provide explanation: Information is for identifying public users. Public users can review/search the P-TACTS documents/filings/proceedings without logging into the system. Public users have read only access to the documents. Public users create their own account from the P-TACTS website.
☒	Obligation to Protect Confidentiality	Provide explanation: 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). This system is governed by The Privacy Act of 1974, which prohibits the disclosure of information from a system of records absent of the written consent of the subject individual.
☒	Access to and Location of PII	Provide explanation: The information captured, stored, and, transmitted by the P-TACTS system is accessible by internal USPTO users. Some of the information is also available to the public and may contain PII, such as Decision documents and Powers of Attorney. The servers storing the potential PII are located in a highly sensitive zone within the USPTO internal network and logical access is segregated with network firewalls and switches through an Access Control list that limits access to only a few approved an authorized accounts.
☐	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.)

Potential threats to privacy include insider threats, unauthorized access and unauthorized changes to confidential and sensitive information, which includes Personally Identifiable Information (PII). In order to combat this threat, P-TACTS is configured to send system and security logs to the OCIO Command Center (C3), whose administrators review and analyze the logs generated in real time for any inappropriate or unusual activities, such as unauthorized system access, unauthorized remote access, or unauthorized configuration settings change, on a daily basis, and report any findings of inappropriate or unusual activity to authorized P-TACTS personnel such as the System Owner Administrators or Technical Leads. If there is any inappropriate or unusual activity, P-TACTS authorized personnel will create a CRQ and take appropriate action to address these activities. Additionally, administrators may adjust the level of review, analysis and reporting if there is a change in the risk to organization assets or operations based on law enforcement information, intelligence information or other credible sources of information. Furthermore, P-TACTS documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII. In addition, the Perimeter Network (NSI) and Security and Compliance Services (SCS) provide additional automated transmission and monitoring mechanisms to ensure that PII information is protected and not breached by any outside entities. P-TACTS uses encryption to encrypt data in transition. Access to PII information is restricted to authorized personnel only.

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.