Privacy Impact Assessment Summary

About the Program

As part of its Intellectual Property Strategy, the Government of Canada created the College of Patent Agents and Trademark Agents, an arm's-length regulatory body intended to regulate the patent and trademark agent profession. The College was established under the *College of Patent Agents and Trademark Agents Act* ("*CPATA Act*"), which received royal assent in 2018 and was proclaimed into force on June 28, 2021.

As an independent regulator, CPATA protects the public interest by strengthening the competencies of patent agents and trademark agents, and building confidence in accessible, ethical and expert intellectual property services in Canada. Our commitment to supporting the rigour and sophistication of the profession plays an important part in driving innovation and stimulating Canada's economic growth.

The College is responsible for protecting the public interest by:

- Setting competence standards for the profession and administering entry requirements that address those standards;
- Implementing the Code of Professional Conduct established by the Minister of Innovation, Science and Industry;
- Administering a fair and open process to respond to concerns about the competence or conduct of agents;
- Establishing expectations for liability insurance, continuing professional development, and pro bono requirements; and,
- Promoting innovation in the delivery of patent and trademark services.

As a new regulatory body, the College anticipates it will take several years to be fully operational. The College is taking a phased approach, focusing on key regulatory infrastructure requirements and processes.

To help accomplish its responsibilities under the *CPATA Act*, the College has engaged a third-party service provider to implement a cloud-based licensee management

solution and several different technology vendors to assist the College in meeting its mandate.

The overall objective of this PIA is to analyze the privacy impacts and risks associated with the proposed design and implementation of several different technology companies and third-party vendors, as well as the supporting CPATA's processes to determine whether the handling of personal information related to such operations is authorized under the *Privacy Act*.

Scope of the PIA

The scope of this PIA encompasses the collection, use, disclosure, retention, and handling of personal information by CPATA. This PIA also identifies high-level privacy considerations related to application and registration, examinations, complaints, investigations, and discipline processes.

Summary of Privacy Issues and Mitigation Strategies

The PIA identified four low privacy risks, and five medium privacy risks, with their respective recommendations for mitigation.

Risk description	Privacy risk	Risk mitigation action plan
Weaknesses in the vendor security safeguards (Penetration Test methodology and response)	Medium	CPATA acknowledges that third party penetration testing can be used to reduce risks when using a software as a service provider. However, it is only one preventative tool, and both CPATA and the vendor have processes in place to maintain high levels of security. Moreover, third party penetration testing is expensive, and a point in time initiative rather than an ongoing risk mitigation strategy. Therefore, there is no short-term plan to engage the licensee database vendor to perform a penetration test. CPATA continues to assess the risks of using vendor software

Risk description	Privacy risk	Risk mitigation action plan
		services and appropriate strategies to reduce risk.
Personal information collected, used, disclosed, or stored on CPATA's behalf by its IT service provider may not be appropriately protected in compliance with the *Privacy Act*.	Medium	CPATA has engaged legal counsel to develop a contract with the IT vendor. The vendor has signed a document that stipulates appropriate privacy and security provisions as recommended.
Licensees may not be notified when their name-change request is denied.	Medium	Mitigations are in the process of being implemented. CPATA is developing a name-change policy to help address this risk.
CPATA does not have a security policy in place, nor is it subject to the TBS Policy on Government Security	Medium	A Security Policy is planned for development in 2024.
Limited audit logging capabilities within the third-party vendor platform for CPATA staff	Medium	CPATA is reviewing its privacy training content to ensure this topic is clearly addressed and plans to roll out an auditing process in future.
Contracts with SaaS vendors do not require privacy breach notification.	Low	CPATA has determined that updates to contracts with CPATA's main SaaS vendors are not required.
'Contact information' is not defined under the *CPATA Act*, Regulations, by-laws or in the *Privacy Act*	Low	CPATA is currently in discussions as to how best address this (timelines not yet determined).

Risk description	Privacy risk	Risk mitigation action plan
Lack of authority for collection of some personal information through the criminal record check process.	Low	CPATA has developed a decision-making framework for the collection and use of personal information and will apply this framework to the collection of personal information through the criminal record check process to ensure compliance with the Privacy Act and TBS policy.
Weakness in third-party vendor platform authentication controls (concurrent sessions and timeout)	Low	CPATA will ensure this topic is addressed in annual privacy training for employees.