May 19, 2026

The Honourable Gary Anandasangaree
Minister of Public Safety
269 Laurier Avenue, West
Ottawa, Ontario K1A 0P8

The Honourable Sean Fraser
Minister of Justice and Attorney General of Canada
284 Wellington Street
Ottawa, Ontario K1A 0H8

Mr. Paul Cardegna, Clerk of the House of Commons Standing Committee on Public Safety and National Security

RE: Bill C-22, An Act respecting Lawful Access and Supporting Authorized Access to Information

Dear Ministers Anandasangaree and Fraser and Members of the Standing Committee on Public Safety and National Security,

On behalf of the Canadian Chamber of Commerce, I am writing to share our proposed amendments for Bill C-22, *An Act respecting Lawful Access and Supporting Authorized Access to Information*.

The Canadian Chamber of Commerce is the country's largest business association with a network of over 400 chambers of commerce and boards of trade representing nearly 200,000 businesses of all sizes, in all sectors and regions of our country. We are grateful for the broad collaboration across Canadian industry in developing these proposals.

In short, Canadian industry is very concerned with this legislation. We are concerned that if implemented, C-22 Part II could push industry away from investing and growing in Canada. Our concerns focus on the fact that this legislation will weaken cyber security safeguards, undermine and even break encryption, and force companies to place their digital systems and our personal information at risk. These measures and anticipated industry reaction to them, undermines our broader efforts to encourage investment and economic growth in Canada.

These risks are not abstract. In their letter on May 7, 2026, the Chairs of the U.S. House Judiciary and Foreign Affairs Committees called Bill C-22 "a dangerous precedent that could erode the mutual benefits of strong encryption standards," and "fracture global cybersecurity norms and weaken our collective defenses against malicious actors who exploit inconsistent standards."

With so many risks facing the Canadian economy, the weight of the measures in C-22 Part II is overwhelming and would undermine Canada's security and competitiveness at a critical time in our history. We are pleased to see the government has signaled some openness to changes, as we much prefer to propose than oppose.

It is in that spirit and to give ourselves a two-track ability to achieve results, we urge you to split C-22 and allow Part I to proceed in Parliament on an expedited basis. This will enable Parliament and industry to collaborate over the summer and fall to refine C-22 Part II into something more realistic and implementable, without the significant risk it currently poses to Canada's economy and our national security.

We also recommend you add a mandatory parliamentary review to both Part I and Part II, requiring the government to return to Parliament after 3 years to demonstrate how these measures have been used and what impact they've had on industry and on reducing and responding to crime in Canada.

We offer our amendments, and industry technical representatives are standing by to provide you and your officials with any information that you may need.

Amendments to Part I

Split C-22 Part I from C-22 Part II: Allow C-22 Part I to proceed in Parliament with the following amendments:

Scope of access to computer data: Remove or narrowly constrain language permitting access to data "available to" a device to ensure warrants remain targeted, avoid broad or general searches to remote data, and mitigate Charter and cross-border legal risks.

Production Order Thresholds: "Reasonable grounds to suspect" is an unreasonably low standard, particularly given the Supreme Court of Canada's findings regarding high potential sensitivity of subscriber information. Amend Part 1 to replace "reasonable grounds to suspect" with "reasonable grounds to believe".

Timeline for Responding to Production Orders: Amend Part 1 to restore 30-calendar-day default as is the case for the Criminal Code standard; shorter periods are most welcome with written judicial reasons in exigent circumstances.

Cross-border Data Sharing: Amend Part to add mandatory comity and conflict-of-law analysis; prohibit enforcement where compliance contravenes provider's home jurisdiction laws; require consideration of bilateral mechanisms (e.g., CLOUD Act Executive Agreement).

Amendments to Part I and Part II

Add a mandatory Parliamentary Review after 3 years: Add a new section applying to both bills that requires a mandatory parliamentary review within 3 years of coming into force.

Direct requests: Require that public safety officials seek information and content data directly from the person or organisation under investigation, rather than the service provider, unless an independent judge determines that doing so would compromise the investigation (for example, by risking evidence destruction or flight). This approach preserves due process, promotes public trust and transparency, reduces unnecessary third-party disclosure, and limits systemic risk. This is also the direction given by the US Department of Justice to US law enforcement authorities.

Conflict of Laws: Introduce relief (e.g., an exemption or legal defence) or at minimum a comity analysis where compliance with Canadian law would place companies in violation of their legal obligations in other jurisdictions where they operate. A secret order under Part II could compel a Canadian company to take action that violates the GDPR, UK Data Protection Act, the Australian Privacy Protection Act, and equivalent regimes. Non-disclosure obligations may also result in cases where a Canadian firm with international operations is required to contravene foreign laws and regulations, and the Canadian firm will be precluded from seeking relief from the foreign regulator on a path forward.

Amendments to Part II

Remove Section 5 and Section 7, all corresponding subsections: The obligations outlined in this section are the source of many in industry's concerns. They place incredible requirements on businesses of all sizes and in many industries, and, by their very definition, weaken encryption. These sections should be removed.

Recommendation (Judicial authorization): Clarify that a warrant is required for the proposed authorities exercised under Part II, including sections 5, 7, 14, and 20.

Recommendation (Scope of application): Anchor the definition of "electronic service provider" to a primary function test, ensuring obligations apply only to entities whose core business is the conveyance of communications between persons.

Recommendation: (Data retention): Remove the requirement for broad, long-term metadata retention mandates. Instead, use targeted, time-limited preservation orders for specific metadata when needed (modelled on the existing preservation-demand framework in section 487.012 of the Criminal Code), to reduce costs and security risks and section 8 *Charter* violations. For context, the EU Court of Justice has repeatedly found general and indiscriminate retention of metadata to be incompatible with fundamental rights, and the United States imposes no general mandatory data retention requirement.

Recommendation (Exigent circumstances): Clarify and appropriately limit the expansion of warrantless access under section 487.11 to ensure thresholds remain high and well-defined.

Recommendation (Transparency and accountability): Require annual public reporting to Parliament on the use of "Confirmation of Service" demands and other authorities under the Act.

Recommendation (Purpose clause): Strengthen the purpose section of Part II to clearly reflect the dual objectives of enabling lawful access while protecting data security and privacy.

Recommendation (Judicial review): Ensure that judicial review is clearly available across all relevant provisions.

Recommendation (Compliance timelines): Introduce flexibility in timelines to comply with non-exigent requests.

Recommendation (Cost recovery): Require a clear, fair cost-recovery framework so that companies are fully compensated for compliance costs (implementation, maintenance, and operations). Each order should specify compensation terms and payment timelines to prevent undue financial burdens on providers.

Recommendation (Legislative clarity): Clarify the relationship between this Act and existing provisions in the Criminal Code and explain the removal of intercept-related provisions from C-22.

Recommendation (Authorized Person) Only law enforcement and government authorized representatives should be empowered to use the powers in this legislation. . Current wording indicates that a designated individual may enter any place for the purpose of verifying compliance with the Act, including examining any computer, system, document or electronic data. Reasonable restrictions around the time, place and method of such inspections, in addition to clarifying who is authorized to see these sensitive systems, should be codified in legislation.

Recommendation (Foreign legal demands for Canadian public sector data): Introduce “blocking statute” language to prohibit the disclosure by any person or entity of Canadian public sector data required as part of any foreign legal proceedings, absent the public sector body’s consent or a bilateral agreement.

Recommendation (Jurisdictional limits): Limit the application of the Act to Canadian facilities, equipment, and persons.

Recommendation (Government due diligence): Before the government and commissioner, acting independently, make an order under Part II, they must each be independently confident that such a request would not cause a systemic vulnerability. The government should also establish a clear mechanism for providers to challenge or decline orders that would undermine security, even where the order may not meet the high statutory threshold for "systemic vulnerability", without penalty while such a challenge is under review.

Thank you for your consideration. We would be pleased to meet at your convenience to discuss our recommendations and answer any questions you have.

Sincerely,

David Pierce

Vice-President, Government Relations