TECHNATION CA

The Honourable Jean-Yves Duclos P.C., M.P.
Chair, Standing Committee on Public Safety and National Security
House of Commons, Ottawa
K1A OA6

Re: Bill C-22: An *Act Respecting Lawful Access*

Dear Mr. Chair,

TECHNATION is Canada's leading technology association. Our members encompass Canadian large companies and SMEs, multinationals and innovators who contribute to enhancing Canada's economic growth and global competitiveness through technology.

We would like to commend the Government for its ongoing commitment to keeping Canadians safe and supporting law enforcement with the tools they need to fight crime in an increasingly digital world. TECHNATION is supportive of the end objective of Bill C-22 and we are encouraged by the improvements from its previous iteration, most notably within Part 1 of the current bill. TECHNATION members are committed to building safe and secure products and believe it is critical to foster this work without introducing vulnerabilities into products and services that create security risks for users.

Strong encryption and the protection of personal, business, and government data are vital to both our economic resilience and our national security posture. TECHNATION members have articulated cybersecurity, and consumer protection concerns for end users arising from this bill, including:

Technical Assistance Obligations and the Definition of Systemic Vulnerability (Part 2.5(2)(b))

The technical assistance obligations in Part 2 remains a significant concern. As drafted, they could require service providers to build or maintain capabilities that break, weaken, or circumvent encryption – including introducing third party or government-controlled surveillance tools. Undermining the efficacy of the best security tools available in this way would impact the safety, privacy, and security of all users, and make systems more attractive targets for malicious actors. The primary protection against these risks outlined in Part 2 is to enable providers to challenge demands that would introduce a "systemic vulnerability." However, the definition of systematic vulnerability is unclear.

Recommendations: Strengthen the definition of systemic vulnerability and explicitly clarify that the law cannot require forced decryption capabilities, or other measures that would weaken encryption or authentication.

Metadata Retention (Part 2, Section 5(2))

As written, Part 2 opens the door to regulations authorizing mandatory metadata retention requirements. These provisions could require companies to collect and store sensitive information about users who are not suspected of any wrongdoing. Bulk retention of metadata creates privacy risks, increases exposure to data breaches, runs counter to modern best practices, and could lead to conflicts of law for providers.

Recommendation: Remove the broad retention authority or consider replacing it with a narrowly tailored "preserve on demand" framework for transmission data. Such a framework should be limited to specified categories of metadata, available only on a reasonable suspicion standard tied to a specific investigation, time-bound, and subject to independent judicial authorization for any extended retention.

Core Providers (Part 2, Sections 2(1), 5)

Bill C-22 authorizes the issuance of a technical assistance order on any Electronic Service Provider (ESP), irrespective of their primary function. It also outlines a subset of ESPs that are most likely to be targeted by a technical assistance order called core providers which is defined as an electronic service provider belonging to a class to be set out in a subsequent schedule. This is a significant delegation of authority as it would allow the government to expand the category of core providers after Royal Assent without the same degree of legislative scrutiny that would apply if the affected classes were specified in the bill itself.

Recommendation: Limit the issuance of technical assistance demands to core providers only. Also, incorporate the schedule defining core providers into the Act itself or set out clear statutory criteria and guardrails governing designation.

Prohibition on Disclosure (Part 2, Section 15)

Bill C-22 would impose a broad non-disclosure obligation to maintain the confidentiality of Ministers' orders, including against disclosing the existence or contents of that order, the fact the provider is subject to it, and related exchanges, except as permitted under the Act. The non-disclosure framework is overly broad and risks becoming a default secrecy rule if Canadian authorities rely on secret orders over public regulations, undermining public trust and transparency relating to the core provider's services.

Recommendation: Limit any non-disclosure obligation to circumstances where the requesting authority can demonstrate, based on specific facts, that disclosure would jeopardise the conduct of a specific investigation; limit the duration of the non-disclosure obligation, subject to extension only by a justice or judge; and clarify that the non-disclosure obligation does not prevent general reporting on the existence or nature of demands in aggregate (e.g., transparency reporting that does not identify a specific order or investigation).

TECHNATION CA

Absence of Critical Safeguards and Legal Certainty for Providers

The bill does not impose a limitation on the Government that would prevent the approval of a technical assistance demand on a provider that could *introduce* a systemic vulnerability. This omission leaves the onus of identifying and challenging any systemic vulnerabilities entirely on service providers.

Moreover, in the event a provider must challenge a demand, the bill does not provide any details on the process, timeline, or liability for non-compliance pending adjudication. This creates legal uncertainty and would discourage providers from contesting demands. This omission will undermine the bill's most essential safeguard, as well as the trust and confidence of Canadian internet users in the security of their digital services.

Recommendations: Require due diligence be conducted by the Minister and considered by the Intelligence Commissioner to ensure a technical assistance demand would not result in a systemic vulnerability. Also, codify details about the process and timeline for providers to challenge a problematic demand, and establish liability protections for provider non-compliance while a challenge is pending.

TECHNATION believes the recommendations above would address the most significant outstanding concerns with Part 2. As Parliament continues its consideration of C-22, we strongly encourage the Government to engage collaboratively with industry stakeholders, technical and academic legal experts, and civil society to equip law enforcement with the updated tools necessary to address evolving public safety threats, while safeguarding the privacy and security of digital systems.

Sincerely,

Kevin d'Entremont - President and CEO, TECHNATION

cc: The Honourable Gary Anandasangaree, Minister of Public Safety

cc: The Honourable Sean Fraser, Minister of Justice and Attorney General of Canada