TECHNATION^CA

TO:
Honourable François-Philippe Champagne
Minister of Innovation, Science and Industry of Canada

Honourable Marco Mendicino
Minister of Public Safety

April 4, 2023

RE: Submission of TECHNATION regarding Bill C-26: *An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*

Honourable Ministers,

On behalf of our membership, we are writing today to emphasize TECHNATION's concerns with Bill C-26, *An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*. We agree wholeheartedly with the government's intent to protect Canadians from cyber threats but are concerned that Bill C-26 brings in novel, excessively broad powers under the guise of cybersecurity.

TECHNATION has served as the authoritative national voice for Canada's $230 billion information and communications technology (ICT) industry for more than 60 years. Our membership ranges from large multinational platforms to cutting-edge domestic tech companies and our top ten largest companies collectively employ over 92,000 Canadians in every region of the country.

Reliability of Canadian telecommunication industry

Before turning to the substance of our concerns, we have heard statements by Ministers that Bill C-26 will grant the authority "needed" to secure the reliability of Canada's telecommunications networks. We do not understand how this bill will improve the reliability of Canada's networks. Government intervention in networks is unnecessary – the memorandum of understanding (MOU) signed by the leading telecommunication companies is more than sufficient to manage future blackouts the size and scale of that which struck Rogers Communications in July 2022.

TECHNATION's Concerns with the Telecommunications Act Amendments

After reviewing Bill C-26, we are concerned with the extent of the new powers the government intends to grant itself. These novel powers are without serious limit and present a very real risk not only to our members, but to Canadians.

Our concerns are five-fold:

a. Extent of the Section 15 powers
b. No compensation for complying with Section 15 orders
c. No due diligence defence against AMPs levied under Section 15
d. Broad discretion to make Section 15 orders secret
e. Impaired ability to defend the interests of a shareholder against government overreach.

1. Extent of the Section 15 powers

The extent of the Section 15 powers goes far beyond what is necessary to achieve the government's sought objectives. The power to order telecommunications service providers to "*do anything or refrain from doing anything*" is a novel power that exceeds any existing power.

The government should implement a proportionality test for these powers to ensure the government does not enact highly interventionist policies to mitigate trivial risks. Australia's *Security of Critical Infrastructure Act, 2018 (SCSA)* establishes such a test, which prevents government overreach.

The government should also amend Bill C-26 to require the *advice* and *consent* of an industry-government body of experts, like the Canadian Security Telecommunications Advisory Committee (CSTAC), before implementing highly interventionist policies. Expert civilian oversight such as engaging these experts will act as an additional safeguard for Canadians.

2. No compensation

The lack of compensation for damages or costs incurred when complying with a Section 15 order is confusing to the industry. The government has made clear it intends to use these powers to ban certain vendors, which will impose costs potentially in the billions on Canadian companies. If these companies had acted in a malfeasant manner or deceived Canadians, perhaps this could be justified. However, the equipment the Government of Canada seeks to ban *was vetted and approved* by the government itself for use in Canadian networks.

Further, in the future, the government may seek to use these orders in a fashion which requires compensation. Without the option to grant compensation, the government is missing an opportunity to work with industry in favour of a heavy-handed approach.

TECHNATION recommends the government amend Bill C-26 to provide for compensation at the Minister's discretion or in appropriate circumstances.

3. No due diligence defence for Section 15 AMPs

The due diligence defence is an established section in the *Telecommunications Act* that provides relief for companies that exercised a duty of care to comply with orders but were unable to through no fault of their own.

Canada is currently seeing record inflation, thanks in large part to challenges with global supply chains. Labour is in very short supply across the country, especially in trade. The consequence of not providing a due diligence defence for AMP levied under orders requiring both technology from overseas and substantial labour input is, at best, inexplicable.

TECHNATION recommends the government amend Bill C-26 to include the due diligence defence for all Section 15 orders.

4. Broad discretion to make Section 15 orders secret

There are certain circumstances where the government would be right to make a Section 15 order in secret. However, the broad power to make these orders secret without oversight offers the government the opportunity to make orders secret with the sole purpose of *concealing its actions not from Canada's enemies, but from Canadians themselves*.

There is an easy solution. The government should amend Bill C-26 to require the Minister to make an application to the federal court requesting that an order be kept secret and that the court be required to balance the rights of Canadians to know what their government is doing with the government's purported need to conceal its actions.

TECHNATION regards the government's broad discretion to make Section 15 orders as highly inappropriate and in need of serious constraint to prevent abuse.

5. Impaired ability to defend shareholder's interests

The novel judicial review rules go beyond, to our understanding, what currently exists in Canadian national security law. Even in the most sensitive circumstances, like security certificate cases, counsel with security clearances are permitted to review the evidence before their clients.

What the government has proposed is, without exaggeration, the ability to *present secret evidence in secret hearings*, and have the judge issue a decision without the applicant even knowing about the existence of the evidence.

We believe the justice system should *privilege transparency above all else*. The government should constrain – or eliminate – these rules and focus on maximizing transparency for Canadians.

TECHNATION's Concerns with the CCSPA

TECHNATION supports the government's efforts to improve cybersecurity for critical industries. But as drafted, the CCSPA is deficient in several respects:

1. No inter-industry sharing provisions.
2. No proportionality required for cybersecurity directions.
3. Excessively broad definitions of "cybersecurity incident" and "critical cyber system"
4. Unrealistic and unworkable deadline for providing notice of a cyber security incident.

1. No inter-industry sharing provisions

Today, many industries manage, mitigate, and respond to cyber threats through groups like the Canadian Cyber Threat Exchange (CCTX). These groups are trusted as forums for cyber professionals to discuss sensitive information. Bill C-26 will undermine the existing threat management infrastructure that exists and replace it with a slower, government-managed alternative.

Bill C-26 should create "safe harbours" protection for organizations and individuals and thereby encourage them to share experiences and resiliency plans, among other important threat management information.

2. No proportionality required for cyber security directions

As TECHNATION noted above for Section 15 orders, no proportionality is required for cybersecurity directions either. This means that the government can exercise an inordinate amount of power to respond to trivial threats -- which present a clear threat to the privacy and safety of Canadians.

As discussed above, the government should amend C-26 to require proportionality in how the government responds to cyber threats with directions.

3. Excessively broad definitions of "cybersecurity incident" and "critical cyber system"

The definitions provided in C-26 for "cybersecurity incident" and "critical cyber system" are excessively broad in that they lack any materiality threshold and lend themselves to multiple interpretations -- which may affect both how the government exercises its powers, as well as how and how much information is reported by companies.

The government should amend "cybersecurity incident" so that a reportable incident arises only when there is a malicious material interference with the continuity or security of a vital service or vital system or the confidentiality, integrity or availability of the critical cyber system. It should be made clear that an imminent, but not actual, interference is not included (as has been made clear in the comparable legislation in the United States, the *Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA))*.

The government should amend "critical cyber system" so that it applies only to a cyber system that, if its confidentiality, integrity or availability were compromised, ***would*** affect the continuity or security of a vital service or vital system ***in one or more material ways***.

Without these changes, C-26 will result in ***excessive overreporting of incidents***, placing an unwarranted regulatory burden on industry and making it harder for the Communications Security Establishment and regulators to identify and quickly respond to critical incidents.

4. Unrealistic and unworkable deadline for providing notice of a cybersecurity incident

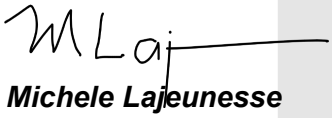
The deadline in the CCSPA for providing notice of a cybersecurity incident is "*immediately*". This timeframe is both ***unrealistic and unworkable***. The government should amend C-26 so that a designated operator must report a cybersecurity incident in respect of its critical cyber systems within ***72 hours of it reasonably believing*** that a reportable incident has occurred. This change will align the CCSPA with CIRCIA in the United States.

Conclusion

TECHNATION strongly agrees that cybersecurity should be a top priority for the government, as well as a top priority for Canadians. However, governments must get this right. We are deeply concerned with deficiencies in Bill C-26 and the potential impact this could result on the conversation around cybersecurity and the role of the government to keep Canada cyber secure. We are specifically requesting to reduce the scope of the powers seeking to grant the government with Bill C-26. Our members are concerned – and a greater risk to updating Canada's cyber laws, we expect Canadians will be concerned too.

We urge you to reconsider and constrain the powers to protect Canadians from government overreach.

Thank you for the opportunity to submit this commentary.



Michele Lajeunesse
Senior Vice-President, Government Relations & Policy

About TECHNATION

As a national industry association, TECHNATION is the industry-government nexus for technology prosperity in Canada. As a member-driven, not-for-profit, TECHNATION unites Canada's technology sector, governments, and communities to enable technology prosperity in Canada. TECHNATION champions technology prosperity by providing advocacy, professional development and networking opportunities across industry and governments at all levels; connecting Canadian scale-ups with global tech leaders; engaging the global supply chain; and filling the technology talent pipeline.

TECHNATION has served as the authoritative national voice of the $230 billion ICT industry for over 60 years. More than 44,000 Canadian ICT firms create and supply goods and services that contribute to a more productive, competitive, and innovative society. The ICT sector generates more than 671,100 jobs and invests $8.0 billion annually in R&D, more than any other private sector performer. For more information: www.technationcanada.ca. TECHNATION was formerly the Information Technology Association of Canada (ITAC).