November 27, 2023

Standing Committee on Public Safety and National Security
House of Commons, Parliament of Canada

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

As Canada's largest business association, the Canadian Chamber of Commerce is pleased and thanks you for the opportunity to submit comments for consideration on Bill C-26 (An Act Respecting Cyber Security – ARCS). Cyber security is essential in ensuring the digital economy's viability, operation, and growth and is vital to furthering innovation and securing trust in our data-driven world. This is why the Canadian Chamber of Commerce and its Cyber. Right. Now. Council was pleased to see Bill C-26 proceed to committee for study.

Canada is facing an increasingly complex and risk-prone digital landscape; with a cyber security skills gap of some four million people globally and an ever-increasing number of connected devices (67 billion devices and counting), the challenges and costs associated with securing our digitally-enabled world are increasing. Every organization in every industry sector risks a cyber breach, but few carry the same real-world risk from cyberattacks as those in the critical infrastructure sector. This threat will only grow as our critical infrastructure increasingly relies on software and connected technology to power and support their operation. However, amendments are needed to ensure the full potential of Bill C-26 and that both the government and industry are not overwhelmed with new or duplicative responsibilities and compliance measures required by the bill. As an example, as currently written, the Bill will overwhelm the government and industry with reports of cyber security incidents unless reportable cyber security incidents are better defined.

Apart from the Personal Information Protection and Electronic Information Act (PIPEDA) and related obligations, Canada has no regulations to govern critical infrastructure operators and owners to report, prepare for, and prevent cyber security incidents. In April 2023, a Russian-linked hacking group successfully penetrated a Canadian natural gas pipeline provider and was "…able to increase valve pressure, disable alarms, and make emergency shutdowns." Ports, marine and ferry facilities have a regulatory obligation to report cyber incidents to law enforcement and Transport Canada. Still, there is no specific reporting period or guidance on the cyber security measures they should implement, making Bill C-26 a positive step forward.

Securing Canadian critical infrastructure from threats is a shared priority between industry and the government. This is why Bill C-26 must develop a cyber security regime in cooperation with industry that reduces risk and recognizes due diligence norms to ensure a standardized and predictable process to improve cyber security across Canada.

We thank you in advance for considering our input into Bill C-26. We welcome your comments and questions and gladly make ourselves available at your convenience to meet to discuss Bill C-26 further.

Kind regards,

**Ulrike Bahr-Gedalia**
Senior Director, Digital Economy, Technology & Innovation and Cyber. Right. Now. Council Lead Canadian Chamber of Commerce
**C: 613.410.6629 E: ubahr-gedalia@chamber.ca**

1700 - 275 Slater Street, Ottawa, ON K1P 5H9 | info@chamber.ca
Chamber.ca @CdnChamberofCom

# Annex

To ensure that Bill C-26 can have the most meaningful impact on improving Canadian cyber security, amendments are needed to strengthen security in the nine policy objectives identified in the Act. The amended bill will allow the government, through the Governor in Council or Minister of Industry, to take steps to secure telecommunication systems in the case of a threat, interference, manipulation, or disruption.

## Part 1: Telecommunications Act

Bill C-26's proposed amendments to the Telecommunications Act would provide for ministerial orders that can ban telecommunications service providers (TSPs) from using any specified product or service in relation to their network or facilities. Moreover, it can direct a TSP to remove any specified product from its network or facilities, impose conditions on the use of any product or service, and impose conditions on a telecommunications service provider's provision of services to a specified person. The Canadian Chamber of Commerce is not against these in principle but stresses a need for the inclusion of due diligence, due process and parliamentary oversight that is present elsewhere in Bill C-26.

### A. Due diligence defence for violations resulting in monetary penalties

**Recommendations:**

- Delete Section 72.132: "A violation that is continued on more than one day constitutes a separate violation in respect of each day during which it is continued."

- Add to Section 72.133: "(b) any evidence that the person exercised due diligence to prevent the violation;"

- Delete from Section 72.15: "other than a violation under section 72.131,"

Reasoning: Section 72.13 does not consider due diligence regarding preventing violations within the determination of the administrative monetary penalty (AMP) levied against companies that are non-compliant with the Act. As drafted, these AMPs are punitive, and existing language and explanations from the Government have caused confusion and reinforce that AMPs are punitive. There may be cases when a service provider cannot fully comply with an order due to circumstances beyond their control. If a service provider has taken all reasonable steps to comply with an order, due diligence should be an acceptable defence, as it is for other violations. Due diligence exists throughout the act in various aspects and procedures, and its addition to this section falls in line with the intent of the Act.

Section 72.132 outlines that a continuous or extended violation of the Act can be met with additional fines daily. As non-compliance is often related to systemic issues that are not quickly resolved within a day, a single continuous violation of the act could result in substantial and repeated monetary penalties. Such strict penalties could cause widespread outages of telephony, Internet, and mobile services due to insufficient time to adequately develop and test fixes, which could have unintended technical vulnerabilities. Removing Section 72.132 would still allow the recognition of separate violations without diminishing the government's ability to levy fines for ongoing violations.

### B. Ministerial Order Making Power

**Recommendations:**

- Delete Section 15.1(6):
  "No one is entitled to any compensation from Her Majesty in right of Canada for any financial losses resulting from the making of an order under subsection (1)."

- Add after Section15.1(5):
  "(6) The Minister may, in accordance with the regulations made, provide fair and reasonable compensation to any person for losses suffered as a result of the application of section 15.1, 15.2, or regulations made under 15.8(1)(a)."

- Delete Section 15.2(7):
  "No one is entitled to any compensation from Her Majesty in right of Canada for any financial losses resulting from the making of an order under subsection (1) or (2)."

- Add after Section 15.2(6):
  "(7) The Minister may, in accordance with the regulations made, provide fair and reasonable compensation to any person for losses suffered as a result of the application of section 15.1, 15.2, or regulations made under 15.8(1)(a)."

- Revise to make Ministerial orders public by default unless reasonable grounds are provided to make an order secret.

- Require the Minister to consult with the Canadian Security Telecommunications Advisory (CSTAC) before making ministerial orders that could significantly impact industry.

Reasoning: A ban on discretionary compensation in the event of financial losses from the making of an order is unnecessarily restrictive and ineffective. Amendments to Sections 15.1 and 15.2 would afford the Minister greater flexibility in ministerial order making as a policy tool. This revision would afford the Minister considerable discretion to evaluate whether providing compensation for parties complying with an order is appropriate. If a ministerial order is indeed meant as a seldom-used policy tool, allowing the minister's discretion in applying compensation would provide the Minister with a means to counteract any negative ramifications of a ministerial order, not just the affected party. Further, retaining the Minister's ability to compensate at their discretion is also likely to increase industry engagement by reducing the perception that ministerial orders are a punitive tool.

While there are many instances in which orders need to be kept secret to protect national security, the powers of the Minister to make any order secret, without checks and balances, risks damaging trust in government. The secrecy provisions of Bill C-26 could be made more focused by requiring, as a default, that such orders be issued publicly unless the Minister reasonably believes that publication is likely to increase the cyber security threats to the telecommunications system or the TSP subject to such an order. Furthermore, in the case of judicial review, the Minister has the power to order that critical information be withheld from an applicant and their legal counsel. This raises serious doubts as to whether procedural fairness can be maintained. Amendments should, at a minimum, allow the disclosure of secret information to a special advocate during judicial review.

The Canadian Chamber of Commerce submits that the Government of Canada should first work with TSPs to conduct an impact assessment of removing any given technology or service under the act to identify unintended consequences such as service degradation or the creation of new security concerns before such orders are made. Given that the intent of the law is to strengthen the security of our

telecommunications infrastructure and that service availability is a key objective, consulting with providers in advance should be a necessary step, particularly given the substantial administrative and monetary penalties proposed for non-compliance. Requiring the Minister to consult with CSTAC would provide greater predictability in risk and potential impacts in the event. This consultation will increase trust between industry and government and enable the Minister to make orders with a better understanding of the risks involved and the potential impacts on service providers affected by an order.

The proposed changes to the Telecommunications Act in its current form could negatively impact Canadians. These include decreased service reliability, increased costs due to unexpected equipment replacement without reimbursement and a potential degradation in trust in government and telecommunications service providers due to the secrecy provisions of the legislation preventing proper public awareness. While creating a transparent cyber security regulatory regime and standards for telecommunications industry firms is beneficial, the uncertainty created around equipment removal, patching and secrecy could undermine the security improvements achieved through these measures. The National Security and Intelligence Committee of Parliamentarians should be able to review any secret orders made by the minister within a reasonable timeframe to ensure proper accountability and transparency. Such orders should be made available to the public by default after six months unless publicly ordered by the Minister.

## Part 2: Critical Cyber Systems Protection Act (CCSPA)

### A. Better define a reportable "cyber security incident"

There should also be greater clarity as to which Orders in Council, Ministerial orders, or regulations could address specific types or severity of security threats. The Canadian Chamber of Commerce is concerned that without a better definition, industry could be forced to report many security events that do not pose a material threat to a vital system or the integrity availability of critical infrastructure. This would undermine the purpose of C-26 and overwhelm government authorities, who will have to process and assess each cyber incident reported.

Currently, the Act provides the Minister with an undefined scope of authority. As such, the Canadian Chamber of Commerce recommends developing a more precise definition of what constitutes a "cyber security incident" and what kinds of incidents CI operators/owners should report, including clear parameters for determining when/if an incident is reportable. The Canadian Chamber of Commerce recommends the following definition as a starting point: cyber security incident, in respect of a critical cyber system, means an incident, including an act, omission or circumstance, that jeopardizes or may imminently jeopardize interferes or may interfere with:

- the continuity or security of a vital service or vital system; or
- the confidentiality, integrity or availability of the critical cyber system.

The Canadian Chamber of Commerce also recommends including "materiality" and risk-based standards, such that incidents would only become reportable where a critical cyber system's actual or potential threat to security, confidentiality, integrity, or availability is material. There is a potential adverse effect on the security of the system and/or information contained in the system.

### B. Recognize the interconnectedness and interdependency of CI systems, infrastructure and software

Concerning Vital Services and Vital Systems (Section 6 and Schedule 1), as well as the Designated Operators of Critical Cyber Systems (Section 2 definitions. Section 7/8 and Schedule 2), Bill C-26 must recognize the interconnected and interdependent nature of multiple CI systems, infrastructure and software that could produce cascading impacts should one system fail. The Government of Canada must establish clear and transparent criteria that consider the importance of the system/service/operator in the context of CI.

**C. Software supply chain**

Given CI's interdependent and increasingly software-defined nature, the government should prioritize strengthening the security of software used to operate CI, IT networks, Operational Technology (OT), and Internet of Things (IoT) devices and systems. The software supply chain involves a complex web of dependencies with numerous third-party developers, components, and providers. In many cases, CI operators have little knowledge of the software components embedded in their control systems.

**D. There is a need to better define the "record keeping" obligations under the Act**

There should be greater clarity to Section 30 (2) and not defer to any upcoming regulations. As currently written in the Act, "…records must be kept in Canada by the designated operator that is at any place that is prescribed by the regulations — or, if no place is prescribed, at the designated operator's place of business…" Without additional clarity, this obligation may be impossible for many designated operators to achieve. Given that the physical address of such operators does not equate to any data residency in Canada, this obligation leaves much to interpretation. Therefore, the Canadian Chamber of Commerce recommends seeking additional clarity vis-à-vis residency of records.

**E. Immediate reporting of cyber security incidents**

The CCSPA proposes "immediate" reporting of a cyber security incident in accordance with the regulations. This is not realistic as following a cyber incident, organizations must first undergo initial stages of an investigation to determine the nature, maturity, and scope of the incident before it can be reported. Requiring reporting "within 72 hours" would be reasonable and harmonizes with existing reporting regimes, such as in the United States.

**F. The CCSPA should be harmonized with pre-existing obligations**

To avoid overlap and conflict, the government should harmonize the CCSPA's requirements with existing obligations, including cyber security requirements in the United States. Harmonizing the Act would significantly reduce compliance costs and enable designated operators to dedicate greater resources to incident prevention activities.

**G. The CCSPA should encourage meaningful two-way information sharing**

The CCSPA only contemplates one-way information sharing from designated operators to the government. No provision is made to provide designated operators access to government information or encourage greater information sharing between designated operators. This is a missed opportunity. To facilitate the sharing of classified threat intelligence, designated operators' cyber security personnel should also be granted expedited access to security clearances.

**H. Personal liability could exacerbate Canada's cyber security talent shortage**

Holding individuals personally liable for activities during their employment may make it more difficult for designated operators to attract and retain the cyber security personnel needed to protect their critical cyber systems. Personal liability should be narrowly scoped to protect the due diligence of designated operators in executing their work and be limited to criminal behaviour and negligence.