**Ashar S. Ahmed, BCSc, MSc, SSCP, CC**

**Oct 24, 2024**

**Senator Tony Dean**
Chair, SECD Committee
Senate of Canada
Ottawa, ON, K1A 0A4

**Senator Jean-Guy Degenais**
Vice Chair, SECD Committee
Senate of Canada
Ottawa, ON, K1A 0A4

**Subject: Urgent Need to Pass Bill C-26 to Enhance Cybersecurity and Improve Public Service Delivery**

---

**Dear Senators Dean and Degenais,**

I hope this letter finds you both in good health and spirits. I am writing to you as an American-Canadian Systems Security and Cyber Security Practitioner with prior experience in our public service related to cyber security, concerned about the present state of our national digital security landscape.

**The discourse around Bill C-26 has been marked by disagreements and controversy, largely due to the concerns about potential centralization of power and privacy issues that may arise from its enactment. As a professional deeply involved in the cybersecurity sector, I am firmly convinced that the importance of passing this legislation far surpasses these concerns.**

A cyber attack occurs globally every 39 seconds, underlining the critical urgency to strengthen our defences against such threats, which are growing in complexity and potential harm. Cybersecurity is not simply a localized issue for technologically developed economies; it is a global one, and Canada **must** be at the forefront of tackling it.

The recent creation of the Department of Cyber Security and Digital Solutions in Nova Scotia[1] reflects the growing need for services that are swiftly responsive, effectively tailored, and conveniently delivered.

---

[1] *New Department to Focus on Digital Services, Programs. Government of Nova Scotia.* ***https://novascotia.ca/news/release/?id=20230524001.***

This department is a pioneering step in transforming how services are delivered and improving cybersecurity in the province, a feat that Bill C-26 can emulate on a federal scale.

However, it is essential for all parties to engage in collaborative dialogue, find common ground, and address the concerns while maintaining the spirit of the legislation. To address these concerns while preserving the spirit and objectives of Bill C-26, I've proposed a set of amendments centred around the following principles:

**Power Authorized**: This aspect empowers the Minister or a designated officer, in consultation with the CSE, to direct a telecommunications service provider to take specified actions to secure the Canadian telecommunications system. This gives the government the necessary authority while maintaining safeguards against undue interference.

**Data Protection Standards:** The proposed amendment emphasizes adherence to existing Canadian data protection laws, such as *PIPEDA*, which should alleviate concerns about privacy and misuse of data.

**Transparency and Accountability:** Provisions requiring written explanations for orders, stakeholder consultations, and public disclosures strengthen accountability and should dispel concerns about unchecked power.

**Appeal Process:** The proposed amendment provides an appeal process to the NSIRA, which would serve as a vital check on government authority and ensure that orders are justifiable and proportionate.

In closing, I implore you and all members of the SECU Committee to focus on the critical importance of Bill C-26 for our nation's cybersecurity and public service delivery. The risks of delaying or diluting this legislation are far too great. Please consider my suggestions, and work diligently towards a consensus that will lead to enhanced digital security and improved service delivery for all Canadians.

Thank you for your time and consideration. I am confident that under your leadership, our nation will navigate toward a secure and efficient digital future.

Respectfully,

**Ashar S. Ahmed, BCSc, MSc, SSCP, CC**
Systems Security / Cyber Security Practitioner

**Order**

*Start of inserted block*

(2) The Minister, or a designated officer authorized by the Minister, may, in consultation with the Communications Security Establishment (*CSE*), by order, direct a telecommunications service provider to do anything or refrain from doing anything — other than a thing specified in subsection (1) or 15.1(1) — that is specified in the order and that is, in the Minister's or designated official's opinion, necessary to secure the Canadian telecommunications system, including against the threat of interference, manipulation, or disruption. In the order, the Minister or designated official may, among other things,

(a) prohibit a telecommunications service provider from using any specified product or service in, or in relation to, its telecommunications network or telecommunications facilities, or any part of those networks or facilities;

...

(l) require that a telecommunications service provider implement specified standards in relation to its telecommunications services, telecommunications networks or telecommunications facilities.

**Data Protection Standards**

(5) In collaboration with the Communications Security Establishment (*CSE*), the Minister or designated official shall ensure that the management of information obtained from telecommunications service providers adheres to data protection standards in compliance with existing Canadian data protection laws, including the Personal Information Protection and Electronic Documents Act (*PIPEDA*).

**Transparency and Accountability**

(4) The Minister or designated official shall ensure transparency and accountability in the decision-making process by:

(a) providing a written explanation of the rationale for the order, including an assessment of the potential risks, benefits, and impact on the affected telecommunications service provider;

(b) regularly reviewing and updating the order to ensure its continued necessity and proportionality in relation to the intended purpose;

(c) consulting with relevant stakeholders, including the affected telecommunications service provider, prior to issuing or amending the order, unless doing so would undermine the purpose of the order;

(d) publicly disclose a summary of the order, subject to the limitations necessary to protect sensitive information and national security concerns.

**Appeal Process**

(3) A telecommunications service provider may appeal an order issued under subsection (2) to the National Security and Intelligence Review Agency (NSIRA) as an independent review board. The NSIRA shall have the authority to review the order, hear from both the Minister or designated official and the affected telecommunications service provider, and determine if the order is justified based on the evidence presented while taking into consideration transparency and accountability requirements. The NSIRA shall issue a decision within a specified timeframe, and its decision shall be binding.

*End of inserted block*