
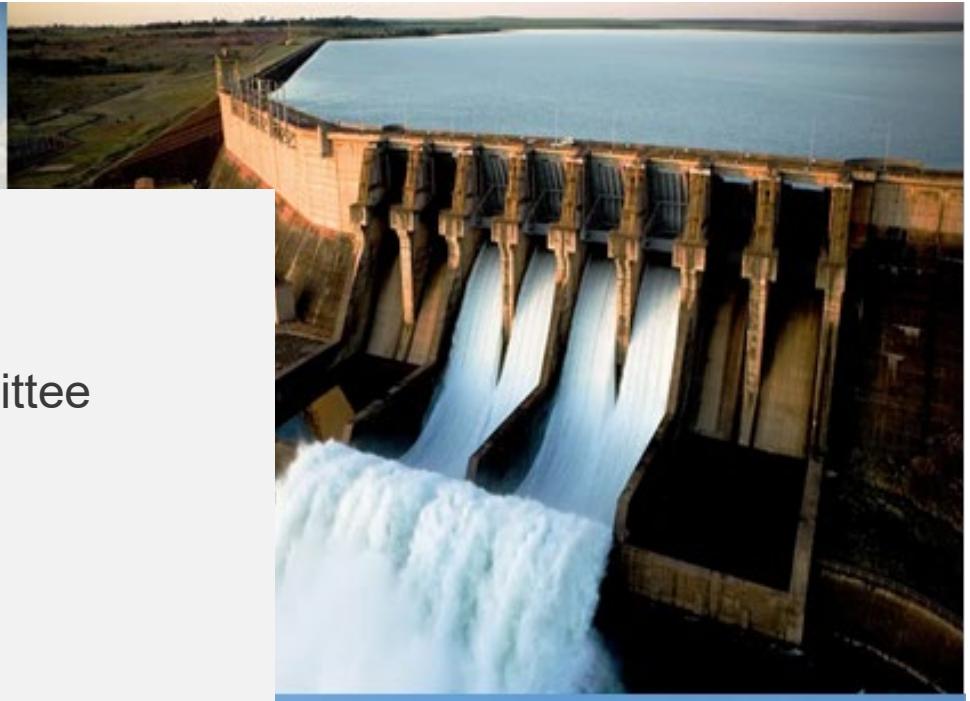

Senate Standing Committee on Public Safety and National Security
Re: Bill C-26

November 2024

National Centre for Critical Infrastructure Protection, Security and Resilience

NC-CIPSeR

Briefing Note: Enhancing Cybersecurity for Canada's Critical Infrastructure

To: Senate Standing Committee on Public Safety and National Security

From: National Centre for Critical Infrastructure Protection, Security, and Resilience (NC-CIPSeR)

Date: November 11, 2024

At the National Centre for Critical Infrastructure Protection, Security, and Resilience (NC-CIPSeR), we are deeply concerned about the rising trend in cyber-attacks targeting critical infrastructure. Canada must view these incursions for what they are – threats to national security.

NC-CIPSeR supports the proposed amendments to the Telecommunications Act and the establishment of the Critical Cyber Systems Protection Act (CCSPA) as outlined in Bill C-26. Notably, the inclusion of a national reporting mechanism to track cyber events in Part 2 will provide crucial insights to help secure the four critical sectors moving forward.

This brief offers recommendations for the implementation of Bill C-26 and outlines key next steps to enhance Canada's cybersecurity resilience. Recognizing the urgency of timely action on this matter, NC-CIPSeR urges the Senate to pass Bill C-26 as written.

The National Centre for Critical Infrastructure Protection, Security, and Resilience (NC-CIPSeR)

NC-CIPSeR is a Canadian federal not-for-profit organization dedicated to enhancing the protection, security and resilience of critical infrastructure (CI) across the nation. Our mandate is to provide actionable research, expert guidance and education, while fostering strategic collaboration with government, industry and academia to enhance the security and resilience of Canada's critical infrastructure. We maintain a particular focus on addressing evolving hazards and threats such as cyberattacks, climate change, and physical disruptions.

Strengthening Canada's Critical Infrastructure: The Role and Urgency of Bill C-26

NC-CIPSeR sees Bill C-26 as the natural evolution of Canada's work to harden Canada's (CI). Due to the interconnected nature of the four sectors (Transportation, Telecommunications, Finance and Energy), disruptions—whether from natural disasters, physical disruptions or cyber incidents—can trigger widespread, cascading effects, underscoring the urgency and need for effective protection and coordination.

Canada's commitment to CI protection was first established through the National Strategy for Critical Infrastructure and the National Cross Sector Forum 2021-2023 Action Plan for Critical Infrastructure. Both promote a collaborative approach among federal, provincial, and private partners. These frameworks prioritize resilience, risk assessment, and response coordination.

The National Cyber Threat Assessment (NCTA) 2025-2026 highlights the escalating threat landscape, specifically noting the increased prevalence of Cybercrime-as-a-Service (CaaS) and the heightened risks posed by state-sponsored actors like China and Russia. The 2025-2026 assessment underscores that ransomware and advanced hacking tools continue to target Canadian CI, underscoring the need for the proactive, adaptable cybersecurity policies contained in Bill C-26.

Furthermore, the Office of the Auditor General's 2021 review of Canada's CI cybersecurity practices identified several gaps in federal coordination, incident response, and resilience

measures. Public Safety Canada's 2024 mid-term progress report echoed this, and positions Bill C-26 as an integral piece within the broader framework of Canada's CI resilience strategy.

Recommendations for Bill C-26

NC-CIPSeR supports Bill C-26's objectives to safeguard Canada's CI from cyber threats, and provides the following recommendations for strengthening Bill C-26 through implementation strategies:

1. Integration of Emerging Technologies

Integrate mechanisms for periodic updates to compliance requirements, drawing on models like the U.S. Cross-Sector Cybersecurity Performance Goals, and the Canadian Nuclear Safety Commission's Design Basis Threat (International Atomic Energy Agency Guidelines) baseline approach. This will ensure that Bill C-26 remains adaptable to rapidly advancing technologies such as artificial intelligence (AI), high-performance computing (HPC), and quantum-resistant cryptography.

2. Adoption of Zero Trust Architecture

Mandate the adoption of common Zero Trust Architectures profiles across the four critical infrastructure (CI) sectors to reinforce cybersecurity defenses against sophisticated, evolving threats. Such guidance is aligned with Five Eyes conversations and some commitment and will help safeguard against complex and evolving threats.

3. Implement Compliance Education

Prioritize Continuing Professional Development (CPD) for front line CI professionals including Operators, Information Technology, Risk Managers and Procurement (supply chain) groups, to facilitate compliance. Providing resources, training, and best practices driven by evidence-based research, will foster a security-oriented culture and reduce reliance on punitive measures, making compliance more accessible, collaborative and effective.

4. Fund Canadian Risk Metrics

Invest in dedicated research for cybersecurity, policy, business continuity, risk assessments, and critical infrastructure interdependencies. Further research related to performance metrics, such as response times and incident reduction rates, to measure the effectiveness of Bill C-26 and compliance regulations over time. Tracking these metrics will allow for informed, evidence-based adjustments to the regulatory framework as technology and threats evolve.

5. Integrate Five Eyes Best Practices

To ensure Canada's CI cybersecurity measures are aligned with Canada's commitments to Five Eyes allies, investment is needed to enhance our capabilities under Bill C-26. Canada must leverage its Five Eyes partnerships to incorporate tested frameworks and advanced practices that other member nations have implemented. This includes Australia's standards for incident reporting and resilience, U.S.-style Zero Trust mandates and memory-safe programming, and the UK's newly updated, sector-specific guidelines.

Bibliography

Australian Government. (2021). Security Legislation Amendment (Critical Infrastructure) Act 2021. Retrieved from Security Legislation Amendment (Critical Infrastructure) Bill 2021 – Parliament of Australia.

Australian Government. (2023). Critical Infrastructure Resilience Strategy. Retrieved from critical-infrastructure-resilience-strategy-2023.pdf

Canadian Centre for Cyber Security. (2024) National Cyber Threat Assessments Retrieved from National Cyber Threat Assessment 2025-2026 - Canadian Centre for Cyber Security

CISA. (2023). Cross-Sector Cybersecurity Performance Goals. Retrieved from Cross-Sector Cybersecurity Performance Goals (CPGs) | CISA

Government of Canada. (2024). Critical 5 – Adapting to Evolving Threats: A Summary of Critical 5 Approaches to Critical Infrastructure Security and Resilience. Retrieved from 2024-dptng-vlvng-thrts-en.pdf

Government of Canada. (2024) Five Eyes Joint Reports. Retrieved from Joint advisory on exploring memory safety in critical open source projects - Canadian Centre for Cyber Security and Exploring Memory Safety in Critical Open Source Projects | CISA

International Atomic Energy Agency. Design Basis Threat. Retrieved from https://www.iaea.org/topics/security-of-nuclear-and-other-radioactive-material/design-basis-threat

Macaulay and Bhasker. (2024). High Performance Computing Infrastructure and Zero Trust Architecture. Retrieved from High Performance Computing Infrastructure and Zero Trust Architecture | Pulse & Praxis: The Journal for Critical Infrastructure Protection, Security and Resilience

Office of the Auditor General of Canada. (2024). Combatting Cybercrime. Retrieved from Report 7—Combatting Cybercrime

Parliament of Canada. (2021). C-26. An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts. Retrieved from C-26 (44-1) - LEGISinfo - Parliament of Canada

Public Safety Canada. (2024). Disruptions on the Horizon; Retrieved from PH4-198-2024-eng.pdf

Public Safety Canada. (2022). National Strategy for Critical Infrastructure: What We Heard Report. Retrieved from PS4-296-2022-eng.pdf

Public Safety Canada. (2024). National Cyber Security Strategy 2019-2024: Report on the Mid-term Review. Retrieved National Cyber Security Strategy 2019-2024: Report on the Mid-term Review

Public Safety Canada (2009, 2010, 2023). National Strategy for Critical Infrastructure; Action Plan for Critical Infrastructure. Retrieved from National Strategy for Critical Infrastructure

Public Safety Canada (2021). National Cross Sector Forum: 2021-2023 Action Plan for Critical Infrastructure.
Retrieved from 2021-ctn-pln-crtcl-nfrstrctr-en.pdf

SecurityWeek. (2023). Guidance on Memory Safety; Retrieved from Five Eyes Agencies Publish Guidance on Eliminating Memory Safety Bugs - SecurityWeek

The White House. (2021). Executive Order on Improving the Nation's Cybersecurity. Retrieved from Executive Order on Improving the Nation's Cybersecurity | The White House

UK Government. (2022). Guidelines from the National Cyber Security Centre on sector-specific cybersecurity standards. Retrieved from National Cyber Security Centre - NCSC.GOV.UK

National Centre for Critical Infrastructure Protection, Security and Resilience
Care of Carleton University, 1125 Colonel by Drive, Ottawa, ON, K1S 5B6