New Federal Cybersecurity Legislation Applicable to Energy Companies and Banks is on the Horizon

By John Sanche, Chelsea Nimmo, Mardi McNaughton, Sadhna Mathrani, Eva Cooper and Lily Yao

Cybersecurity threats pose a great risk to businesses, individuals, and national security. On June 18, 2025, Parliament tabled Bill C-8, *An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts* (Bill C-8).[1] If passed, Bill C-8 would introduce new cybersecurity requirements for Canadian critical cyber systems in the federally regulated sector and telecommunications systems.[2] Part 1 introduces cybersecurity amendments to the existing *Telecommunications Act*,[3] while Part 2 proposes to enact the new *Critical Cyber Systems Protection Act*.

Proposed *Critical Cyber Systems Protection Act*

The preamble to the proposed *Critical Cyber Systems Protection Act* acknowledges that "some cyber systems are critically important to vital services and vital systems", such that any disruptions could have serious consequences for national security and/or public safety.[4] The stated purpose of the legislation includes detecting, identifying, managing, and mitigating cybersecurity risks for critical cyber systems—meaning interdependent digital services, technologies, assets or facilities that form the infrastructure for transmitting, processing or storing information.[5]

The proposed legislation is intended to target businesses regulated by the Canadian Energy Regulator, the Canadian Nuclear Safety Commission, the Ministries of Industry and Transport, the Superintendent of Financial Institutions, and the Bank of Canada.

If passed as drafted, the legislation would require designated operators of critical infrastructure to establish a cybersecurity program to detect security incidents and minimize their impacts,[6] within 90 days of being classified as a designated operator.[7] Once established, such cybersecurity programs would need to be reviewed regularly,[8] and any cyber-related actions would need to be documented.[9] Additionally, designated operators would be required to identify security risks in their supply chain or use of third-party products and services and mitigate these on an ongoing basis.[10] Cybersecurity incidents would need to be reported to the Communications Security Establishment within 72 hours,[11] and contraventions of the legislative scheme could result in administrative penalties, or even imprisonment.[12]

---

[1] Bill C-8, *An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*, 1st Sess, 45th Parl, 2025 (first reading 18 June 2025) [***Bill C-8***].
[2] The predecessor to Bill C-8 was Bill C-26, *An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*, 1st Sess, 44th Parl (first reading 14 June 2022) [***Bill C-26***]. Bill C-26 was in its final stages when the 44th Parliament ended in March 2025, and as such, the legislation was never enacted.
[3] *Telecommunications Act*, SC 1993, c 38 [***Telecommunications Act***].
[4] Bill C-8, Part 2, cl 11.
[5] Bill C-8, Part 2, cl 2 & 5.
[6] Bill C-8, Part 2, cl 9(1).
[7] Bill C-8, Part 2, cl 9(1).
[8] Bill C-8, Part 2, cl 13(1).
[9] Bill C-8, Part 2, cl 30(1).
[10] Bill C-8, Part 2, cl 15.
[11] Bill C-8, Part 2, cl 17.
[12] Bill C-8, Part 2, cl 137.

Proposed changes to the *Telecommunications Act*

Bill C-8 also proposes changes to the *Telecommunications Act* which would generally expand the power of the Governor in Council to make orders relating to telecommunications products or services that pose cybersecurity threats. The amendments propose the introduction of an administrative penalty scheme for violations of any such orders, including penalties of up to $15 million.[13]

What to Expect Moving Forward

In the coming months, we expect to see a great deal of chatter around this topic. While some provinces already have similar legislation for critical infrastructure,[14] this will be a major federal advancement. Bill C-8 is in its early stages and may undergo changes before it is passed.

If you are the operator of critical cyber systems in the federally regulated sector, it would be prudent to begin assessing your current cybersecurity systems. Regardless of the progress and ultimate outcome of Bill C-8, strong cybersecurity measures are necessary more than ever with the rise of AI and expected changes to privacy laws in Canada.

If you are unsure of how your organization will be affected by the proposed legislation or the best way to enhance your cybersecurity, reach out to **any of the authors**.

[13] Bill C-8, Part 1, cl 72.131.
[14] Alberta recently enacted the *Security Management for Critical Infrastructure Regulation*, Alta Reg 84/2024.