Bill C-8 revives Canadian cyber security reform: What critical infrastructure sectors need to know

July 28, 2025

Key takeaways

What's happened?

The Carney government has revived expansive cyber security rules under Bill C-8, which aims to strengthen the compliance requirements for federally regulated critical infrastructure sectors, including banking, transportation, energy, and telecommunications.

Why does it matter?

The cyber protection obligations for "designated operators" that carry out vital services or systems are stringent and broad. Once passed, they'll require organizations to maintain comprehensive cyber security programs; identify material changes to systems (particularly those that have national security implications); and immediately report breaches. Violations could result in fines of $15 million *per day* for organizations.

What can you do?

Critical infrastructure organizations should take proactive steps and engage external resources to help meet the bill's cyber security obligations, which are expected to be passed quickly when Parliament resumes in the fall. These measures include mapping vital systems; understanding new powers of applicable regulators; developing and implementing the necessary plans and training to improve cyber resilience; and, creating capacity to respond to both breaches and ensuing investigations to limit risk and liability.

On June 18, 2025, Bill C-8, *an Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*, was

introduced in the House of Commons to address gaps in the federal government's ability to protect critical infrastructure systems. Bill C-8 notably revives the sweeping cyber security obligations and regulatory powers first proposed under Bill C-26 (which was tabled three years earlier but never enacted).

While largely identical to Bill C-26 (which BLG previously commented on in this June 2022 Insight), C-8 introduces several key changes. These include revised judicial review procedures and the removal of consequential amendments to the *Canada Evidence Act* (aimed at protecting sensitive information filed during judicial reviews or appeals).

Although Bill C-8 has to go through the full legislative process, both its similarities with C-26 and the fact that the predecessor bill almost passed before Parliament was prorogued suggest it could move swiftly through Parliament. Organizations in federally regulated sectors including banking, transportation, energy, and telecommunications should prepare now for these significant changes.

Compliance obligations

The proposed *Critical Cyber Systems Protection Act* (CCSPA) under Bill C-8 imposes onerous cyber security obligations on "designated operators" of federally regulated critical cyber systems. These operators carry out vital services or systems (that is, infrastructure essential to preserving national security and public safety).

These obligations include, among others:

- Developing, maintaining, and regularly reviewing cyber security programs (CSPs);
- Reporting material changes in ownership, control, or use of third-party products and services to the appropriate regulator, as to mitigate supply-chain and third-party risks;
- Complying with cybersecurity directions (CDSs) from the governor in council;
- Reporting cyber security incidents to the Communications Security Establishment (CSE) within 72 hours; and
- Preserving detailed records of cyber security programs and incidents.

Unfortunately, the CCSPA provides limited guidance as the requirements laid out are high-level. Specific obligations – particularly those relating to the establishment, implementation, and maintenance of cyber security programs – will be defined under future regulation. As a result, designated operators must complete a comprehensive inventory of their cyber systems and assess their criticality.

This limited legislative detail is compounded by the government's authority to issue binding (and confidential) cyber security directions. In addition, there is no requirement for the government to consult with designated operators prior to issuing these directions. For instance, a direction could be issued requiring an operator to implement specific security measures, without first consulting them on operational feasibility, cost implications, or service continuity impacts.

Sector-specific oversight & enforcement

A central feature of Bill C-8 is its delegation of broad, sector-specific powers to the appropriate regulator:

- **Banking systems:** Overseen by the Office of the Superintendent of Financial Institutions (OSFI).
- **Clearing and settlement systems:** Overseen by the Bank of Canada.
- **Interprovincial or international pipeline and power line systems:** Overseen by the Canadian Energy Regulator (CER).
- **Nuclear energy systems:** Overseen by the Canadian Nuclear Safety Commission.
- **Telecommunications services:** Overseen by the minister of Industry.
- **Transportation systems within federal jurisdiction:** Overseen by the minister of Transport.

Specifically, Bill C-8 will allow these regulators to:

- Enter any place (including private property, but excluding dwelling houses without consent or a warrant) and examine anything on site, including any record, report, or data;
- Order internal audits of practices, books, and other records;
- Issue binding compliance orders requiring designated operators to cease non-compliant activities or to take corrective measures within a specified timeframe; and
- Request or share information, including confidential information, so long as the minister or responsible minister is satisfied that information deemed confidential is treated as such.

Furthermore, Bill C-8 reintroduces significant administrative monetary penalties (AMPs) for violations. While the proposed regime is designed to promote compliance, fines could amount to $15 million per violation, *per day*, for organizations – and $1 million per violation, *per day*, for individuals. Moreover, directors and officers of designated operators could be held personally liable if they were complicit in committing a violation.

Violations can be contested – for example, by raising a due diligence defence. A compliance agreement could also be entered into with the appropriate regulator. Such agreements may reduce, in whole or in part, the penalty – but would be deemed an admission to having committed the violation. If defaulted on, the full penalty would become payable, and the violation could be made public.

Is your organization ready?

Designated operators should take proactive steps to build robust cyber security programs and practices that will meet the anticipated obligations under Bill C-8. To reduce exposure to potential penalties and strengthen cyber readiness across their operations, critical infrastructure organizations should:

- Assess whether your organization is a “designated operator” under the CCSPA and seek external support in mapping all systems, services, and operations that may be considered “vital.”

- Determine which regulator oversees your compliance with the CCSPA and consider whether pre-emptive discussions on the implications of the bill to your sector would be worthwhile.
- Establish governance frameworks with clear accountability channels, while designating individuals and teams develop and implement the necessary procedures to meet compliance obligations.
- Build internal capacity to respond both to breaches and to subsequent inspections, audits, and compliance orders – including tabletop exercises and live drills.
- Continually assess your obligations in the context of evolving threats and regulatory updates.

Being prepared does not just mean your organization is ready for the likely passing of Bill C-8. It will result in you and your team having a strategic advantage to meet the changing cyber threat landscape.

Contact us

BLG's Cybersecurity, Privacy & Data Protection Group and AI lawyers closely monitor rapidly evolving cyber security and privacy legislation, and can assist you in understanding your organization's obligations and how best to prepare for Bill C-8.

Please reach out to the key contacts below if you have any questions about Bill C-8 and how its adoption may affect your organization.

By

Hélène Deschamps Marquis, Matt Saunders, Chloe Hughes-Légaré, Aaron Grech

Expertise

Cybersecurity, Privacy & Data Protection, Information Technology, Corporate Governance, Banking & Financial Services, Technology, Artificial Intelligence (AI), Transportation, Energy - Oil & Gas, Energy – Power

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 725 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749