

Critical Cyber Systems Protection Act: Bill C-8 is adopted

July 02, 2026

This updated article was originally published in July 2025.

Key takeaways

What's happened?

In 2025, the Carney government has revived expansive cybersecurity rules under Bill C-8, introducing the new *Critical Cyber Systems Protection Act*. The Bill received Royal Assent on June 15, 2026, thereby completing the legislative process. Its provisions will come into force gradually, on a day or days to be fixed by order of the Governor in Council.

Why does it matter?

The cyber protection obligations for designated operators that carry out vital services or systems are stringent and broad. Now that the bill has been enacted, organizations will be required to implement comprehensive cybersecurity programs; report any material changes to their 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 measures should be taken now that the Bill is adopted?

Critical infrastructure organizations should take proactive steps and engage external resources to help meet the bill's cybersecurity obligations. 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 15, 2026, Bill C-8, which introduced the *Critical Cyber Systems Protection Act* (CCSPA), received Royal Assent, thereby completing the legislative process. The government has announced its intention to bring the Act's provisions into force on a

phased basis. The bill was introduced with the purpose of reviving the broad cybersecurity obligations and regulatory powers first proposed under Bill C-26 (which was tabled three years earlier but never enacted).

Organizations in federally regulated sectors, including banking, transportation, energy, and telecommunications, should prepare now for these significant changes.

Main compliance requirements imposed by Bill C-8

The proposed *Critical Cyber Systems Protection Act* under Bill C-8 imposes onerous cybersecurity 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 cybersecurity programs** that: a) identify and manage any organizational cybersecurity risks including risks associated with the designated operator's supply chain and its use of third-party products and services; b) protect its critical cyber systems from being compromised; c) detect any cybersecurity incidents affecting its critical cyber systems; d) minimize the impact of cybersecurity incidents affecting critical cyber systems; and e) do anything that is prescribed by the regulations.
- **Notifying the appropriate regulator of any important changes** in ownership, control or the use of third-party products and services, in order to mitigate supply chain and third-party risks.
- **Mitigating supply chain risks** following, among other things, guidelines developed by the Communications Security Establishment (CSE).
- **Complying with cybersecurity directions from the Governor in Council;**
- **Reporting cybersecurity incidents to the CSE within 72 hours;**
- **Keeping records** respecting any steps taken to implement the cybersecurity program, to mitigate any supply-chain or third-party risks, any measures taken to implement a cybersecurity direction, every cybersecurity incident reported, and any matter prescribed by the regulations.

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 cybersecurity 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) cybersecurity directions.

When issuing such directions, the Governor in Council must ensure that the scope and substance of the provisions contained in the direction are reasonable in relation to the purpose of protecting a critical cyber system. In addition, the Governor in Council must consider factors such as the order's impact on operational activities, public safety of Canadians, privacy of Canadians, delivery of vital services and systems to consumers,

the financial impacts, and any other factor that the Governor in Council considers to be relevant.

Notwithstanding the obligations described above, 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 remains 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 \$500,000 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 must take proactive steps to build robust cybersecurity programs and practices that will meet the obligations under Bill C-8. Is your organization a critical infrastructure? To reduce exposure to potential penalties and strengthen cyber readiness across your operations, your organization 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 new act to your sector would be worthwhile;
- Establish governance frameworks with clear accountability channels, designating individuals and teams to 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 provisions of Bill C-8 to come into force. 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 cybersecurity 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 its potential implications for 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 800 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

The information contained herein is of a general nature and is not intended to constitute legal advice, a complete statement of the law, or an opinion on any subject. No one should act upon it or refrain from acting without a thorough examination of the law after the facts of a specific situation are considered. You are urged to consult your legal adviser in cases of specific questions or concerns. BLG does not warrant or guarantee the accuracy, currency or completeness of this publication. No part of this publication may be reproduced without prior written permission of Borden Ladner Gervais LLP. If this publication was sent to you by BLG and you do not wish to receive further publications from BLG, you may ask to remove your contact information from our mailing lists by emailing unsubscribe@blg.com or manage your subscription preferences at blg.com/MyPreferences. If you feel you have received this message in error please contact communications@blg.com. BLG's privacy policy for publications may be found at blg.com/en/privacy.

© 2026 Borden Ladner Gervais LLP. Borden Ladner Gervais LLP is an Ontario Limited Liability Partnership.