OSLER

Canada's Bill C-8: what businesses need to know about the new cybersecurity framework

JUNE 17, 2026 14 MIN READ

Related Expertise

- Banking and Financial Services
- Cybersecurity and Security Incident Response
- Defence, Security and Aerospace
- Nuclear Energy
- Pipelines
- Privacy and Data Management
- Technology
- Telecom

Authors: Éloïse Gratton, Ad. E., Adam LaRoche, Tina Saban, CIPP/C, Naomi Chernos

Introduction

Bill C-8, *An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*, establishes the most significant federal cybersecurity framework Canada has enacted. The Bill creates a dual regime: it expands the federal government's power to secure Canada's telecommunications system, and it imposes mandatory, enforceable cybersecurity obligations on operators of critical cyber systems across federally regulated sectors.

Bill C-8 is the successor to Bill C-26, which was introduced in the previous Parliament but did not become law before Parliament was prorogued. It was reintroduced last year in substantially similar form as Bill C-8 in the 45th Parliament. The Bill reached a significant milestone on June 16, 2026, when received royal assent. Having now completed its passage through Parliament, the majority of its substantive obligations set out in Part 2 of the Bill will come into force on a day or days to be fixed by order of the Governor in Council, with many operational details to follow by regulation, while the amendments to the *Telecommunications Act* in Part 1 (as described in more detail below) are now in force.

The legislation responds to an evolving threat landscape — rising incident frequency, lateral movement across networks, and the targeting of service providers — and brings Canada's approach closer to those of key allies, including the United States (*Cyber Incident Reporting for Critical Infrastructure Act of 2022* (CIRCIA)), the European Union (NIS2 Directive), and the United Kingdom (Network and Information Systems Regulations 2018 (NIS Regulations)). This Update summarizes the key provisions, their privacy and commercial implications, and practical steps organizations should consider.

Overview and structure

Bill C-8 is divided into two operative parts:

- **Part 1 — Amendments to the *Telecommunications Act*:** Adds the promotion of the security of the Canadian telecommunications system as a policy objective and grants the Governor in Council and the Minister of Industry broad powers to direct telecommunications service providers (TSPs) to take, or refrain from taking, specified actions to secure the system.

- **Part 2 — *The Critical Cyber Systems Protection Act* (CCSPA):** Enacts a new statute establishing comprehensive cybersecurity obligations for "designated operators" of "critical cyber systems" in federally regulated sectors, together with audit, compliance-order, and penalty mechanisms.

A third part provides for a five-year parliamentary review of the provisions enacted or amended by the Act. Together, the two operative parts create a layered regime of obligations, government direction-making powers, and enforcement tools that will materially affect how critical-infrastructure businesses manage cyber risks.

Part 1: Amendments to the *Telecommunications Act*

Part 1 confers significant authority on the Governor in Council and the Minister of Industry to issue security-related orders to TSPs. Section 15.1 permits the Governor in Council to prohibit a TSP from using the products or services of a specified person, or to direct their removal from the TSP's networks or facilities. Section 15.2 gives the Minister a longer list of powers, including prohibiting the use of specified products or services, imposing conditions on their use, requiring termination of service agreements, mandating security plans, vulnerability assessments and standards, and — under a broad catch-all in paragraph 15.2(2)(m) — directing a TSP to do, or refrain from doing, a specified thing.

These powers provide a formal statutory foundation for supplier-exclusion decisions of the kind Canada has previously taken in respect of 5G equipment and significantly expand the government's ability to intervene in TSPs' procurement, vendor-management and network-security decisions on an ongoing basis. The breadth of the authorities conferred by sections 15.1 and 15.2 is therefore one of the most consequential aspects of the legislation.

The exercise of these powers is subject to a number of key features and safeguards.

Key features and safeguards

- **Necessity and proportionality:** Orders must, in scope and substance, be necessary and reasonable in relation to the gravity of the threat. Before making an order, the decision-maker must consider its operational, financial, telecommunications-service, and privacy impacts.
- **Confidential orders:** Orders may include provisions prohibiting disclosure of their existence or contents, subject to a list of factors the decision-maker must weigh, including the impact on transparency and accountability. Secret orders must be notified to the National Security and Intelligence Committee of Parliamentarians and the National Security and Intelligence Review Agency.
- **Firm limits:** The Minister may not order a TSP to intercept a private communication or radio-based telephone communication, or order the decoding of an encrypted private communication, as defined in section 183 of the Criminal Code.
- **No compensation; orders prevail:** Notably, no compensation is payable for financial losses resulting from an order, and an order prevails over an inconsistent CRTC decision to the extent of the inconsistency. Orders are exempt from the Statutory Instruments Act.

Enforcement

Contravention of an order or regulation made under sections 15.1 or 15.2 is a violation subject to administrative monetary penalties (AMPs) of up to **$25,000 for an individual**

(**$50,000** for a subsequent contravention) and up to **$10 million in any other case** (**$15 million** for a subsequent contravention). The same conduct may alternatively be prosecuted as a summary conviction offence carrying fines in the court's discretion and, for individuals, imprisonment of up to two years less a day.

Judicial review is available, but under special rules: the Minister may withdraw evidence from the proceeding, and the designated Federal Court judge must not base the decision on withdrawn material and must keep it confidential. Notably, the Act does **not** establish a special-advocate regime, and amendments that would have required prior judicial authorization for orders were ruled out of order during House consideration. The regime as enacted therefore rests on executive discretion checked by after-the-fact review, annual reporting to Parliament, and notification to national-security review bodies. This design has attracted procedural fairness and *Charter* criticism — in particular, concerns that affected parties may be unable to know or challenge the basis for orders, and that the absence of a special advocate leaves no independent voice to test the government's evidence in closed proceedings.

Part 2: *The Critical Cyber Systems Protection Act*

Part 2 is the centerpiece of the Bill. The CCSPA imposes mandatory cybersecurity obligations on entities that are deemed "designated operators" of "critical cyber systems" and distributes oversight across six sector regulators.

Who is covered

The CCSPA applies to "designated operators" — defined as persons, partnerships or unincorporated organizations belonging to a class of operators set out in Schedule 2. While Schedule 2 is currently blank, these will be classes of operators who own or operate a "critical cyber system", defined as a system that, if its confidentiality, integrity or availability were compromised, could affect the continuity or security of a vital service or vital system. Schedule 1 lists six categories of vital services and vital systems

- telecommunications services
- interprovincial or international pipeline and power line systems
- nuclear energy systems
- transportation systems that are within the legislative authority of Parliament
- banking systems
- clearing and settlement systems

The Governor in Council may add to Schedule 1 any federally regulated service or system it is satisfied is vital to national security or public safety, and may add new classes of operators and assign a regulator for that class, so coverage may expand over time. Oversight is distributed among the Superintendent of Financial Institutions, the Bank of Canada, the Ministers of Industry and Transport, the Canadian Energy Regulator, and the Canadian Nuclear Safety Commission, each with inspection, internal-audit and compliance-order powers over its assigned classes.

To confirm, the obligations under the CCSPA attach only to the operator's "critical cyber systems" — systems whose compromised confidentiality, integrity or availability could affect the continuity or security of a vital service or system. While all operators will, by virtue of their designation, be considered to be responsible for critical cyber systems, not all of an operator's processes will be subject to the requirements under the CCSPA, where those processes cannot be considered to have an impact on any vital system or service. That definition reaches beyond operational technology, so operators will need to make defensible

determinations about which of their systems would be considered subject to these requirements, based on their involvement and impact on the categories of vital systems and services (which are generally considered to fall within "critical infrastructure"), and which requirements under the CCSPA would apply.

Key obligations

- **Cybersecurity programs (section 9):** Within 90 days of becoming a member of a designated class, an operator must establish a cybersecurity program addressing: (a) identification and management of cyber risks, including supply-chain and third-party risks; (b) protection of critical cyber systems from compromise; (c) detection of cyber security incidents; (d) minimization of incident impacts; and (e) any other prescribed matter. The program must be provided to the appropriate regulator within the same window, implemented and maintained, and reviewed at least annually.
- **Supply-chain and third-party risk (section 15):** In addition to the more general obligation under section 9 to manage risks associated with the supply chain and third-party attacks, there is a duty to mitigate such risks *as soon as* they are identified, including by taking steps in line with any guidance issued by the Communications Security Establishment (CSE).This is one of the most operationally demanding requirements. This mandates a level of vendor risk management that many organizations have not yet formalized. Appreciating that many contracts are ongoing, going forward, organizations should ensure that engagements adhere to internationally recognized frameworks and standards on the mitigation of cybersecurity risk in supplier relationships, and provide for appropriate remediation rights.
- **Incident reporting (subsection. 17–18):** A designated operator must report a cyber security incident in respect of a critical cyber system to the CSE within a period to be prescribed by regulation, not to exceed 72 hours. The threshold is broad: a reportable incident is one that interferes *or may interfere* with the continuity or security of a vital service or system, or with the confidentiality, integrity or availability of a critical cyber system. Separately, immediately after reporting to the CSE, the operator must notify the appropriate regulator that a report was made and provide a copy. The Act expressly preserves the *Personal Information Protection and Electronic Documents Act* (PIPEDA), so CCSPA reporting runs in parallel with existing privacy breach-notification obligations.
- **Cybersecurity directions (section 20):** The Governor in Council may direct a designated operator or class of operators to comply with measures necessary to protect a critical cyber system. A direction must be reasonable in scope and substance, and the decision-maker must consider operational, public safety, privacy, financial and service delivery impacts. An operator subject to a direction is prohibited from disclosing the fact or content of the direction except to the extent necessary to comply (ss. 24–25), and the same encryption and interception limits that apply to Part 1 apply here.
- **Record-keeping (section 30):** Operators must keep records in Canada documenting program implementation, reported incidents, supply-chain mitigation steps, measures taken to comply with cyber security directions, and any matter prescribed by the regulations. They also may be subject to audits and compliance verification by their

regulator.

Penalties and enforcement

- **Administrative monetary penalties** of up to **$500,000 per violation for individuals** and **$15 million per violation in any other case**, with each day of a continuing violation treated as a separate violation. These are statutory maximums; penalty amounts for specific violations and the classification of violations will be fixed by regulation.
- **Offences:** Certain contraventions — including failing to establish or implement a program, failing to mitigate supply-chain risk, and breaching a direction's confidentiality — are offences carrying penalties and, for individuals, imprisonment of up to two years less a day on summary conviction or up to five years on indictment.
- **Personal liability:** Directors and officers who direct, authorize, assent to, acquiesce in or participate in a violation or offence are parties to the offence, whether or not the organization is actually proceeded against.
- **Due diligence:** A due diligence defence is available for violations and most offences — which puts a premium on documented, board-visible compliance efforts. The Act also preserves solicitor-client privilege.

The magnitude of these penalties and the availability of a due diligence defence underscore that compliance is intended to be a board-level governance priority.

Privacy law implications

Bill C-8 sits squarely at the intersection of cybersecurity and privacy law. Legal teams should anticipate the following privacy issues.

Information flows to government

Both parts contain broad information-exchange provisions permitting the sharing of information — including confidential information — among federal bodies such as the CSE, the Canadian Security Intelligence Service (CSIS), the Department of National Defence, and sector regulators for purposes connected to orders and regulations.

The Act includes several privacy-related safeguards. These include a requirement to dispose of personal information once it is no longer necessary, restrictions on the collection, use and disclosure of personal and de-identified information beyond what is reasonable in relation to the threat being addressed, and "for greater certainty" provisions confirming that the *Privacy Act* and PIPEDA continue to apply.

Notwithstanding these safeguards, the Office of the Privacy Commissioner and civil-liberties groups raised concerns during the legislative process regarding the breadth of the information-sharing authorities, the volume of information that could flow to government institutions without individuals' knowledge, and the adequacy of oversight mechanisms. As a result, the practical effectiveness of the Act's privacy protections will likely depend significantly on the content of forthcoming regulations and on how the regime is implemented in practice.

Impacts to organizations

Given the overlap and impact of Bill C-8 on areas traditionally governed by existing privacy laws, organizations should consider how to manage these overlapping privacy obligations.

For example, CCSPA incident reporting (to the CSE) overlaps with privacy breach-reporting obligations under PIPEDA. PIPEDA's breach notification regime requires notification to the Privacy Commissioner "as soon as feasible" and notification to affected individuals if there is a "real risk of significant harm." By contrast, the CCSPA imposes a hard ceiling of 72 hours (with the precise period to be set by regulation), a lower threshold (incidents that "may interfere" with a vital service or system), and a different recipient (the CSE, with immediate copy to the sector regulator). Because the Act expressly leaves PIPEDA intact, organizations will need coordinated incident-response processes that satisfy both regimes on their distinct timelines and thresholds, in addition to the increasingly complex suite of breach notification obligations that apply to organizations operating in regulated industries — such as those imposed on federally regulated financial institutions by the Office of the Superintendent of Financial Institutions (OSFI), or those applicable to regulated entities under the federal *Nuclear Safety and Control Act*. Organizations subject to Québec's *Act respecting the protection of personal information in the private sector* (Law 25) will face a further layer of provincial notification requirements with their own timelines.

Additionally, the provisions permitting confidential orders and non-disclosable directions may constrain how, and how quickly, organizations can communicate security decisions to affected individuals and other stakeholders. This tension may present itself in the context of incident notification efforts.

Commercial law implications, practical considerations and action points

Supply chain and procurement

Third-party contracts will need review and, in many cases, renegotiation to add cybersecurity requirements, audit rights, incident-notification provisions and compliance representations. Given the section 15 duty to mitigate supply-chain risk as soon as it is identified, this is a regulatory imperative, not merely best practice. Organizations should begin reviewing and strengthening their supply-chain risk management now, including updating third-party contract terms on cybersecurity, audit rights and incident notification, to support the ongoing duty to mitigate.

Supplier restrictions and stranded assets

The government's power to prohibit or compel removal of specific suppliers' products creates commercial uncertainty and potential stranded-asset risk, compounded by the absence of any statutory right to compensation. Organizations should develop internal protocols for receiving and handling confidential government orders and directions, including the non-disclosure constraints they carry.

Corporate governance and designation

The scale of potential penalties, the personal exposure of directors and officers, and the formal program requirement all call for board-level oversight of cyber governance and regular reporting on risk and compliance status. As a threshold step, organizations should determine whether they are likely to be a designated operator, based on the Schedule 1 sectors and their regulatory profile, and identify which of their systems could qualify as critical cyber systems. They should then conduct a gap analysis of their current cybersecurity program against the five prescribed program elements, recognizing that the 90-day clock starts when the designation order is published. Board-level cyber-governance and reporting mechanisms should be established to demonstrate compliance and support a due diligence defence.

Insurance

The framework may affect cyber-insurance underwriting and coverage. Organizations should review their cyber-insurance coverage in light of the new penalty and remediation exposure, and confirm whether regulatory penalties, compliance costs and government-directed remediation are covered.

M&A and investment

Compliance status will become a material diligence item for transactions involving designated operators — including pending regulatory actions and the cost of remediation — and may be complicated by confidential orders or directions that a target cannot fully disclose. Organizations engaged in M&A and investment activity should incorporate C-8 compliance into their diligence frameworks for transactions involving potentially designated operators.

Cross-border considerations

Operators active in multiple jurisdictions must reconcile C-8 with overlapping regimes, including CIRCIA, the EU NIS2 Directive and the U.K. NIS Regulations.

Incident response and privacy coordination

Organizations should operationalize incident detection and response for the 72-hour CSE reporting window and the immediate regulator notification duty, coordinated with PIPEDA breach obligations. They should also assess the interaction between new cybersecurity obligations and existing privacy compliance programs, including data-minimization and purpose-limitation principles.

Regulatory monitoring

Organizations should actively monitor the implementing regulations, which will define designated operators, reporting thresholds and timelines, program requirements, and penalty amounts. Early engagement with sector regulators and industry groups can help organizations anticipate and prepare for the specific requirements that will apply to them.

Conclusion

Bill C-8 is a watershed in Canadian cybersecurity regulation. For the first time, federally regulated critical-infrastructure operators will face comprehensive, enforceable cybersecurity obligations backed by significant financial penalties and criminal sanctions. While much detail awaits the regulations, the direction of travel is clear, and the foundations of compliance — a robust program, mature supply-chain risk management, effective detection and reporting, and board-level governance — require sustained investment that cannot be built overnight. Organizations in affected sectors should begin preparing now.

Although the legislative framework is now largely settled, important operational uncertainties remain. Many details will be determined through regulations, including which entities will be designated, the specific incident-reporting thresholds within the 72-hour ceiling, and the required elements of cybersecurity programs. Questions also remain regarding the practical scope of the confidential order powers, the adequacy of the modified judicial review process, the interaction of the regime with future federal private-sector privacy reforms, and whether smaller operators within designated sectors will ultimately be subject to materiality or size-based exemptions.

Osler will continue to monitor the progress of Bill C-8 and the development of implementing regulations, and will provide further updates as the landscape evolves.