Bill C-8: A new federal cyber security framework for telecommunications and critical cyber systems

September 21, 2026

Authors

Eric Lavallée

Partner, Lawyer Partner, and Trademark Agent

Guillaume Laberge

Partner, Lawyer

Ghiles Helli

Lawyer

Bill C-8 received royal assent on June 15, 2026. It deserves special attention. The bill marks a shift in our approach to cyber security, giving the federal government the means to respond quickly when a threat is identified. It also requires certain parties to comply with higher standards, and imposes real penalties for noncompliance.

The legislation is structured around two main areas. The first strengthens the *Telecommunications Act* by empowering the Governor in Council and the Minister of Industry to impose specific measures through Orders in Council and Ministerial Orders. The second establishes the *Critical Cyber Systems Protection Act* (the “CCSPA”), targeting vital systems and services.

With these legislative changes, cyber security is emerging from the shadows—it is becoming a matter of governance and compliance. And with the adoption of this Act, technology decisions, supplier management, and responses to cyber security incidents will need to be more robust, better regulated, and duly documented. We believe that organizations that are proactive in preparing their governance and evidence practices, as well as their contingency plans, will be more agile and more credible in the eyes of their clients and partners.

That said, an important distinction must be made from the outset: the amendments to the *Telecommunications Act* set forth in Part 1 are now in force, whereas the CCSPA, as provided for in Part 2, will come into force following one or more Orders in Council. To date, Schedule 2 of the

CCSPA, which is meant to identify the classes of designated operators and their corresponding regulatory bodies, remains blank.

Key takeaways at a glance - Bill C-8 introduces:

> (i) the authority to issue telecommunications orders (that is, Orders in Council and Ministerial Orders);
> (ii) guidelines for a mandatory program for certain critical cyber systems, subject to the CCSPA coming into force and future designations;
> and (iii) strengthened enforcement in terms of information exchange, audits, administrative monetary penalties, and violations.

Part 1 of the Act – Telecommunications: Security becomes the driving force for action

Bill C-8 explicitly enshrines security in Canada's telecommunications policy by adding the objective of "the promotion of the security of the Canadian telecommunications system." It provides the legal basis for measures that are now designed to be direct, swift, and enforceable.

An important element of the Act, both for its application and for defining the nature of the threats it addresses, is the clarification that "interference with or manipulation, disruption or degradation of a telecommunications system include actions of a technical nature that impede the operation of the telecommunications system but do not include the e?ect of lawful expression, persuasion or political debate." The text thus expressly provides room for freedom of expression and lawful public debate.

Part 1 of the Act includes a two-tier enforcement mechanism: **Orders in Council** and **Ministerial Orders** (issued by the Minister of Industry).

Orders in Council

The Governor in Council may issue an Order in Council if they have reasonable grounds to believe that the measure is necessary to secure the system against a threat, and that it is reasonable in relation to the gravity of that threat. Specifically, the order may:

> Prohibit telecommunications service providers ("TSPs") from using the products and services provided by a specified person in, or in relation to, their networks or facilities; or
> Order the removal of products supplied by a specified person.

Bill C-8 imposes a proportionality requirement: the scope and content must be necessary and reasonable in view of the gravity of the threat. The Order in Council takes precedence over any conflicting decisions, orders, or authorizations, including those under the *Radiocommunication Act*. Furthermore, the government does not bear the economic cost—no compensation is payable for financial losses attributable to the Order in Council. This is, in a sense, the "heavy artillery" of the Act.

The Order in Council may also include a prohibition against disclosing its existence or all or part of its content. Before imposing such a prohibition, the Governor in Council must, in particular, consider the extent to which disclosure could undermine the objective of the order, the necessity of the prohibition in light of the nature of the threat, the possibility of limiting its scope, its impact on the transparency and accountability of the Government of Canada, and any representations made by the affected TSPs.

Before issuing the order, the Governor in Council must also consider the measure's operational impact on the affected TSPs, its financial implications, its effect on the provision of telecommunications services in Canada—including the confidentiality and security of telecommunications—as well as its potential impacts on Canadians' privacy.

Ministerial Orders

The Minister of Industry may, by Ministerial Order, impose highly operational measures when they are necessary and reasonable in view of a threat. The order may, in particular:

> Prohibit the use of specific products or services, order the disposal of personal information, and impose conditions on the use and provision of services;
> Prohibit or force TSPs to terminate service agreements;
> Require review processes for networks, facilities, and procurement plans;
> Require security plans, vulnerability assessments, and mitigation measures;
> Require the implementation of standards;
> Require a backup system;
> Prohibit TSPs from providing services to a specified person;
> Order the suspension of the provision of services to a specified person for a specified period;
> Prohibit certain upgrades; or
> Order TSPs to do or refrain from doing any specified act, subject to the limitations provided for by the Act.

As with Orders in Council, the minister must consider the operational and financial impacts, the effect on the provision of services—including the confidentiality and security of telecommunications—and the potential implications for the privacy of Canadians. The minister may not order the interception of a private communication or a radio-based telephone communication, nor the decryption of an encrypted private communication. The Ministerial Order also comes with a provision stating that no compensation will be paid.

The Act also sets forth a specific limitation: the suspension of service to an individual may be ordered only if the order is necessary to secure the Canadian telecommunications system against a threat of a technical nature specified in the order.

Like an Order in Council, a Ministerial Order may include a prohibition on disclosure. Before imposing such a prohibition, the minister must consider comparable factors, including the impact of non-disclosure on the principles of transparency and accountability of the Government of Canada.

Specifics regarding the publication of orders

In principle, Orders in Council and Ministerial Orders must be published in the *Canada Gazette* within 90 days of their issuance, but the minister making the order may specify in the text itself that it need not be published. In addition, incorporation by reference facilitates the integration of technical documents that are subject to change. We can therefore expect this process to adopt international technical standards.

Collection of information by the minister

Bill C-8 provides that the minister may require the disclosure of information if they have reasonable grounds to believe that it is both reasonable for the information to be provided in view of the gravity of the threat and that it is necessary. However, a confidentiality framework is in place for the information provided, particularly when it involves trade secrets or financial, commercial, scientific, or technical information. Personal information and de-identified information are also subject to protective measures.

The text also provides for the exchange of information among various federal authorities, as well as with the provinces, foreign countries, or certain international organizations under written agreements. The scope and content of personal or de-identified information must be reasonable in view of the gravity of the threat. The Act also provides for the disposal of personal or de-identified information

when it is no longer needed.

It should also be noted that personal and de-identified information are deemed to be confidential information for the purposes of Part 1, even if they have not been expressly designated as such.

Part 2 of the Act – The *Critical Cyber Systems Protection Act* (CCSPA)

It is important to note that this part of the Act will not take effect until the date or dates set by Order in Council. Furthermore, its actual applicability will depend on future designations, since Schedule 2 is currently blank. The framework has therefore been adopted, but it has yet to be implemented.

Key concepts: What the Act actually aims to achieve

The CCSPA applies to critical cyber systems as strictly defined by the text, that is, a cyber system that, if its confidentiality, integrity or availability were compromised, could affect the continuity or security of a vital service or vital system. The definition of “cyber system” is intentionally broad. In practice, the Act is therefore not limited to a “network” in the traditional sense; it can encompass platforms, cloud environments, control systems, digital services, and interconnected technical assets, provided that if they were compromised, it could affect a vital service or system.

The version of the text that has been assented to also adds the definition of “internal audit”, which is an independent and objective review conducted in accordance with internationally recognized guidance on professional internal auditing practices. This reinforces the idea that the expected compliance goes beyond simply adopting internal policies and, where necessary, requires structured assurance mechanisms.

How organizations are designated

A “designated” operator that controls, operates, or owns a critical cyber system is required to comply with the provisions of the CCSPA and its regulations pertaining to that cyber system. How are operators designated?

First, “vital services” and “vital systems” are those listed in Schedule 1, namely: 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, and clearing and settlement systems. By Order in Council, items may be modified, or added to or removed from this schedule within the scope of authority provided for by the Act.

Second, the Act includes a schedule—which is currently blank—that allows for the establishment of classes of operators and regulatory bodies responsible for these vital services or systems.

In practice, compliance depends on both the vital service or system in question (Schedule 1) and the operator class in which the organization is classified (Schedule 2).

Cyber security programs: The foundational requirement

At the heart of the CCSPA is the requirement to develop a cyber security program. After being designated through an amendment to Schedule 2, an operator must establish, within 90 days, a program relating to its critical cyber systems.

This program must include measures, in accordance with the regulations, to identify and manage organizational risks (including supply chains and the use of third-party products and services),

protect critical cyber systems, detect incidents and minimize their consequences, as well as any other measures required by the regulations. The program is therefore not merely a policy—it must cover the entire risk management cycle and be amenable to a “compliance” review. This will force organizations and companies to respond quickly when such a designation is made.

The Act also imposes a monitoring mechanism: once the program is established, the operator must notify the relevant regulatory body in writing.

The Act also requires that any such program be updated periodically. Lastly, reporting requirements apply when significant changes occur, including changes to ownership or control, supply chains, and the use of third parties.

This approach transforms cyber security into a governance and maintenance requirement, rather than a one-time project.

Supply chains and third parties: From assessment to mitigation

The CCSPA explicitly emphasizes supply chains. Once the risks related to supply chains and third parties have been identified in the program (paragraph 9(1)(a)), the designated operator is required to mitigate them (section 15). The verb is important: it is not enough simply to “observe” or “monitor”; the law requires an active mitigation effort, which must be demonstrable.

The Communications Security Establishment (the “CSE”) may develop guidelines on mitigating risks associated with supply chains and the use of third-party products and services, drawing on internationally recognized frameworks. The appropriate regulator may also provide the CSE with information—including confidential information—regarding the program or the measures taken, so that the CSE can provide advice, guidance, and services in accordance with its mandate.

For organizations, this signals a convergence between regulatory requirements and technical expectations: managing suppliers, access, updates, software dependencies, and subcontractors is becoming a core component of compliance.

Incident reporting: A requirement for speed and coordination

The CCSPA establishes a requirement to report cyber security incidents to the CSE. Every designated operator must report any cyber security incident involving one of its critical cyber security systems within the prescribed time limits, which may not exceed 72 hours. The definition of “cyber security incident” covers an incident (including an act, omission, or circumstance) that interferes or may interfere with the continuity or security of a vital service or system, or the confidentiality, integrity, or availability of a critical cyber system.

After filing a report with the CSE, the operator must, without delay, notify the appropriate regulatory body and provide it with a copy of the incident report. The text specifies that these obligations do not diminish the obligations arising from the *Personal Information Protection and Electronic Documents Act*.

Cyber security guidelines: The mandatory response tool

The CCSPA provides for a particularly intrusive measure: cyber security directions. By Order in Council, the government may direct any designated operator or class of operators to comply with

any measure set out in the direction for the purpose of protecting a critical cyber system, but only if it has reasonable grounds to believe that the direction is necessary. Before issuing the order, the government must consider the operational impacts, public safety, privacy protection, financial impacts, and the impacts on the provision of vital services and systems. The scope and content must be reasonable in relation to the protection objective, and the operator in question is required to comply.

The law also sets out two explicit limitations: the Governor in Council may not order the decryption of an encrypted private communication or the interception of a private communication or a radio-based telephone communication.

In addition, a safeguard related to awareness has been put in place: an operator cannot be found guilty of contravening the direction unless they were notified of it or reasonable steps were taken to inform them of it. However, it will be important for an operator not to ignore the notifications received, even if they sometimes seem minor.

The operator in question may not disclose the existence or content of a direction except to the extent necessary to comply with it. This requirement has a significant practical impact: it mandates the implementation of a “need-to-know” policy both internally and with respect to suppliers, subcontractors, insurers, and other partners.

Information: Confidentiality, sharing, and removal of personal information

The CCSPA establishes a comprehensive information-sharing framework, in particular to support the making, amending or revoking of directions. For purposes related to the making, amending or revoking of a direction, certain entities may collect and share information—including confidential information—with one another. The law also regulates the disclosure and use of confidential information and provides for exceptions, particularly when disclosure is required by law or necessary to protect vital services, systems, or cyber systems.

“Provable” compliance

The CCSPA requires the maintenance of records covering program implementation, reported incidents, steps taken to mitigate third-party risks, compliance with directions, and any other matters specified by the regulations. These documents must be kept in Canada in accordance with the terms and conditions prescribed by the regulations or, in the absence thereof, by the appropriate regulator. This requirement is central: it transforms compliance into a burden of proof.

The regulatory framework provides for broad audit and enforcement powers, which are exercised by different authorities—the Superintendent of Financial Institutions, the Minister of Industry through inspectors, the Bank of Canada, the Canadian Nuclear Safety Commission, the Canadian Energy Regulator, and the Minister of Transport—depending on the sector. The provisions governing access to premises, the examination of cyber security systems, and the reproduction and temporary seizure of documents and systems are detailed in the CCSPA. Mechanisms for internal audits and compliance orders are in place, depending on the authority. The law prohibits obstruction and the provision of false or misleading information, which underscores the importance of the quality of the information provided.

The version of the text that has been assented to also adds an explicit provision: the CCSPA does not infringe upon solicitor-client privilege or the professional secrecy of lawyers or notaries.

Watch out for penalties!

It should be noted that the law provides for substantial administrative penalties, as well as criminal offences (including imprisonment).

Executives and directors may be considered co-perpetrators of a violation or offence, as the case may be. Ongoing violations can be counted on a day-by-day basis. Under Part 2 of the Act, administrative penalties may reach $500,000 for an individual and $15,000,000 in other cases.

Furthermore, certain violations constitute criminal offences that are punishable, in some cases, either through charges or summary proceedings. Depending on the nature of the violation and whether the offender is an individual, imprisonment may be possible.

How we can assist you in implementing Bill C-8

In particular, we can assist you with the following:

Regulatory positioning

Mapping your exposure (in terms of telecommunications, vital services or systems, and your current or anticipated designation) and establishing a realistic roadmap, prioritized by risk

Responding to the imposed measures

Supporting the receipt, analysis, and implementation of Orders in Council, Ministerial Orders, or directions

Compliance

Establishing or strengthening governance, record-keeping, and internal processes (including requests for information, audits and inspections, and the traceability of decisions)

Third parties and procurement

Reviewing and negotiating contracts and security requirements (including incident reporting, cooperation, audits, subcontracting, corrections, and withdrawal/replacement) and documenting mitigation measures

Incidents and enforcement

Supporting incident response (including triage, notifications, and the preservation of evidence) and managing the risk of penalties and criminal liability, including for executives and directors

Conclusion

In practice, organizations that may be affected would be wise to start preparing now, even though Part 2 of the law is not yet in force. The practical scope of the Act will depend on the CCSPA coming into force, the adoption of implementation regulations, and the inclusion in Schedule 2 of the classes of operators concerned and their corresponding regulators. In the meantime, organizations that begin structuring their governance, documentation, and third-party management now will be

better positioned to adapt quickly once the sector-specific requirements are clarified.