

Bill C-8 Is Now Law: What Canada's Critical Infrastructure Cybersecurity Act Means for Transportation and Logistics Companies

Transportation & Logistics

1 October 2026

On June 15, 2026, *Bill C-8*, formally titled *An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts* received Royal Assent and became law.

The new statute creates a federal framework governing the cybersecurity of critical infrastructure in Canada and identifies operators in the finance, energy, telecommunications, and transportation sectors. For companies operating in transportation and logistics, the new law goes well beyond an aspirational policy statement. It imposes concrete, enforceable obligations that will change how businesses manage cyber risk, report incidents, and structure their commercial relationships.

From Bill C-26 to Bill C-8: A Long Road to Royal Assent

Bill C-8 has been years in the making. Its predecessor, *Bill C-26*, was introduced during an earlier parliamentary session and would have amended the *Telecommunications Act* while introducing the *Critical Cyber Systems Protection Act* ("CCSPA") to strengthen cybersecurity across federally regulated essential infrastructure in the telecommunications, finance, energy, and transportation sectors. *Bill C-26* completed third reading in Parliament but ultimately failed to receive Senate approval due to a drafting error.

The federal government then tabled *Bill C-8* on June 18, 2025, relaunching cybersecurity reform amid a sustained rise in cyber incidents targeting Canadian organizations. Because the substantive provisions remained nearly identical to those in *Bill C-26*, observers expected the *Bill* to pass without significant amendment. It did just that, clearing Senate's third reading on June 4, 2026, and receiving Royal Assent eleven days later.

The passage of *Bill C-8* marks a clear turning point in how Canada approaches cybersecurity regulation. Prior to its enactment, Canada relied primarily on voluntary cybersecurity frameworks, industry guidance, and the general obligations embedded in statutes like the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"). The new law moves Canada toward mandatory, sector-specific cybersecurity regulation, bringing it closer to the approach already taken by the United States and the European Union. For the transportation sector, the shift from voluntary best practices to enforceable legal obligations carries real operational and legal consequences.

Who Is Affected: Designated Operators and Their Supply Chains

The CCSPA targets "designated operators" of federally regulated critical cyber systems and identifies operators across four sectors: banking, telecommunications, energy, and transportation.

In the transportation context, this captures federally regulated carriers and infrastructure operators, meaning entities whose operations cross provincial or international boundaries or that otherwise fall under federal jurisdiction through statutes such as the *Canada Transportation Act*.

The reach of the legislation, though, extends well beyond designated operators themselves. Any company that sells goods or services to a designated operator, whether a technology vendor, a third-party logistics provider, a telematics platform, or a maintenance contractor, should expect incident-reporting duties and supply-chain attestations to be written into their master service agreements. Even companies not directly designated under the CCSPA will face new contractual cybersecurity obligations flowing from their customers' compliance requirements. Transportation companies that serve as vendors to banks, telecoms, or energy firms face a similar exposure from the other direction.

The supply-chain dimension matters greatly for the transportation and logistics industry, which is deeply interconnected with every other sector of the economy. A freight carrier that transports goods for a designated energy operator, or a warehousing company that manages inventory for a federally regulated bank, may find itself contractually bound to comply with cybersecurity standards it had not previously considered.

Core Obligations: What the Law Requires

The CCSPA imposes strict compliance obligations on designated operators of critical cyber systems. While the specific regulatory details will continue to be developed through subordinate regulations and guidance, the Act's core requirements can be grouped into several categories.

Cybersecurity programs. Designated operators will be required to establish and maintain documented cybersecurity programs that address the identification, protection, detection, response, and recovery functions associated with their critical systems. This goes beyond what many transportation companies have traditionally treated as discretionary IT security hygiene, requiring instead a structured, enterprise-level approach to cyber risk management.

Incident reporting. The Act introduces mandatory incident-reporting obligations for designated operators. When a cybersecurity incident occurs that affects, or has the potential to affect, a critical cyber system, the operator must report it to the appropriate federal authority within prescribed timeframes. For transportation companies accustomed to managing incident response on an ad hoc basis, this represents a significant procedural and cultural shift.

Supply-chain security. As discussed above, the legislation creates obligations related to the security of the supply chains that support critical cyber systems. Designated operators will be expected to assess and mitigate risks arising from their vendors and service providers, and to flow cybersecurity requirements down through their procurement and contracting processes.

Compliance and enforcement. The Act provides the federal government with meaningful enforcement tools, including the ability to issue compliance orders and, in cases of non-compliance, impose administrative monetary penalties. The regulatory framework is designed to ensure that cybersecurity is treated as a board-level governance matter, not simply a technical function.

Why Transportation Is Uniquely Vulnerable

The transportation and logistics sector faces cyber risks that are both distinctive and growing in severity. Increasing digitization within the industry means that disruptions could have severe consequences. Modern commercial vehicles are equipped with an array of digital systems, including electronic logging devices (ELDs), GPS tracking, telematics platforms, on-board diagnostic ports, and wireless connectivity features such as cellular, Bluetooth, and Wi-Fi. Each of these interfaces represents a potential attack surface.

Transport Canada has recognized the growing cyber risk posed by connected vehicle technologies and intelligent transportation systems (ITS). A Transport Canada briefing document on ITS cybersecurity warns that an attack on a critical system "could lead to increased congestion, a higher risk of traffic accidents, and disruptions to major transport routes". Where personal data is breached, there are also privacy implications for the public and reputational damage to the organizations involved.[1] Transport Canada's Vehicle Cyber Security Strategy further emphasizes that cybersecurity is "inextricably linked with safety and privacy," and that a collaborative approach is essential among all levels of government, manufacturers, and industry stakeholders.[2]

Practical Steps for Transportation and Logistics Companies

With the law now on the books and subordinate regulations expected to follow, transportation and logistics companies should begin taking concrete steps.

Assess whether you are a designated operator. Companies should determine whether their operations fall within the scope of the Act's designation criteria. Federally regulated carriers and transportation infrastructure operators are the most obvious candidates, but the government may designate additional entities as the regulatory framework matures.



Review and update your vendor and customer contracts. Even if your organization is not itself a designated operator, it is likely that your customers or business partners are or will be. Expect to see new cybersecurity clauses, supply-chain attestation requirements, and incident-notification obligations in master service agreements, vendor qualification forms, and procurement documents. Reviewing and, where necessary, renegotiating these agreements now will reduce the risk of non-compliance.

Invest in cybersecurity governance. Companies should invest in building documented cybersecurity programs, conducting regular risk assessments, and establishing incident response plans that satisfy the Act's reporting requirements.

Train your people. Companies should invest in training not only their IT staff but also their operational and leadership teams on cybersecurity risks, incident-response protocols, and the organization's obligations under the new law.

Monitor regulatory developments closely. The federal government is expected to advance additional privacy and data legislation, including [Bill C-36, An Act to enact the Protecting Privacy and Consumer Data Act, to amend the Personal Information Protection and Electronic Documents Act](#). Transportation companies should track these developments in tandem, as the cybersecurity, privacy, and data governance obligations are increasingly interconnected.

Conclusion

For federally regulated transportation and logistics companies, the takeaway is simple: cybersecurity is no longer optional, and compliance is no longer a matter of internal policy alone. It is now a legal obligation, a contractual requirement, and a condition of doing business. Companies that invest now in understanding and meeting these obligations will be better positioned to protect their operations, their data, and their commercial relationships going forward.

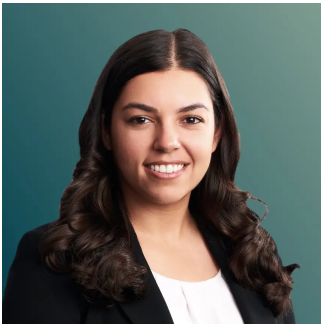
[1] Transport Canada, "Intelligent Transportation Systems (ITS) Cyber Security: Briefing Document" (last modified 17 September 2026), online: Transport Canada <https://tc.canada.ca/en/road-transportation/innovative-technologies/intelligent-transportation-systems/road-infrastructure-cyber-security/intelligent-transportation-systems-its-cyber-security-briefing-document>

[2] Transport Canada, "Transport Canada's Vehicle Cyber Security Strategy" (last modified 17 September 2026), online: Transport Canada <https://tc.canada.ca/en/road-transportation/innovative-technologies/connected-automated-vehicles/transport-canada-s-vehicle-cyber-security-strategy>

(This blog is provided for educational purposes only, and does not necessarily reflect the views of Gardiner Roberts LLP).



Author



Andrea Fernandes

Associate

416.203.9501

afernandes@grllp.com



Bay Adelaide Centre — East Tower
22 Adelaide Street West, Suite 3600
Toronto, ON M5H 4E3

Phone: 416.865.6600
Fax: 416.865.6636
contactGR@grllp.com