JUNE 26, 2025 • 6 MIN READ

Government re-introduces cybersecurity bill for "vital" federal industries

AUTHORS

 Molly Reynolds

 Julie Himo

 Rosalie Jetté

 Nic Wall

 Mavra Choudhry

Last week, the federal government introduced Bill C-8, *An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*. Bill C-8 bears the same title as, and is nearly identical in content to, last Parliamentary session's Bill C-26. This includes the introduction of the *Critical Cyber Systems Protection Act* (CCSPA) and a number of amendments to the *Telecommunications Act*.

What you need to know

- The proposed CCSPA would require organizations in designated "vital systems" or providing "vital services" in the banking, telecom, energy and infrastructure sectors to maintain and regularly review a cybersecurity program, mitigate third-party and supply chain risks, and rapidly report cybersecurity incidents.
- Designated operators would be required to notify their regulator of any material change in their ownership or control or in their supply chain.
- Regulators in these sectors would also be given extensive new powers, including the power to request any information or search any place for the purpose of verifying compliance or preventing non-compliance, and order penalties of up to $15,000,000 for non-compliance with orders and regulations.
- Bill C-8 would also amend the *Telecommunications Act* to give the Minister of Industry the power to prohibit a telecommunications service provider from using products or services provided by, or from providing certain products or services to, a person specified by the Minister.
- Companies subject to these requirements should ensure that they understand them, and that they are positioned to meet them and mitigate related risks.

Scope of CCSPA

The proposed CCSPA imposes obligations on certain classes of organizations that provide services or operate systems that are "vital" to national security or public safety. The presently designated Vital Services and Vital Systems are as follows:

- 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

Most obligations under the CCSPA would apply to "designated operators" within these sectors that own, control or operate a "critical cyber system". While no classes of designated operators are listed in the current draft, a cyber system would qualify as a "critical cyber system" where "if its confidentiality, integrity or availability were compromised, could affect the continuity or security of a vital service or vital system".

Obligations for designated operators

Under the CCSPA, a designated operator would be required to:

- establish a cybersecurity program in respect of its critical cyber systems soon after becoming a designated operator;
- include in its cyber program reasonable steps to (i) protect its critical cyber systems from being compromised, (ii) detect cybersecurity threats and incidents, and (iii) minimize the impact of cybersecurity incidents that occur;
- identify and take reasonable steps to mitigate supply chain and third-party risks;
- notify the appropriate regulator of any material change in the designated operator's (i) ownership or control, or (ii) supply chain or use of third-party products and services;
- regularly review and improve its cybersecurity program;
- report any cybersecurity incident in respect of any critical cyber systems to the Communications Security Establishment (CSE) within a period to be determined by regulations (which will not be greater than 72 hours), then immediately notify the appropriate regulator of the incident; and
- maintain records documenting compliance with CCSPA obligations.

Additional obligations may be imposed by regulation.

CCSPA enforcement

Bill C-8 grants extensive powers to designated regulatory authorities to enforce the requirements of the CCSPA. Currently, the designated regulatory authorities include the Office of the Superintendent of Financial Institutions, the Minister of Industry, the Bank of Canada, the Canadian Nuclear Safety Commission, the Canadian Energy Regulator and the Minister of Transport. Their powers include the authority to:

- request any information or search any place for the purpose of verifying compliance or preventing non-compliance;
- order designated operators to conduct internal audits and report the results;
- issue compliance orders and enter into compliance agreements; and
- order penalties of up to $15,000,000 for non-compliance with orders and regulations.

Amendments to the *Telecommunications Act*

Bill C-8 would also amend the *Telecommunications Act* to give the Minister of Industry the power to prohibit a telecommunications service provider from using products or services provided by a specified person, or from providing certain products or services to a specified person. Such orders would only be made if there are reasonable grounds to believe that they are necessary to secure the Canadian telecommunication system against any threat, and such orders must be proportionate to the gravity of the threat. As under the CCSPA, penalties for non-compliance would be as high as $15,000,000.

Takeaways for companies

While Bill C-8 has only just been introduced, companies governed by the *Telecommunications Act* and that are likely to be subject to the CCSPA should be as proactive as possible with respect to three matters in particular.

First, companies should give significant consideration to how they will protect information subject to solicitor-client, litigation, and other legal privileges. Protecting privilege could be particularly challenging in the event of a cybersecurity incident given the extensive enforcement (including search and seizure) powers afforded to regulators, the record-keeping requirements imposed on designated operators to demonstrate compliance, and the requirement to immediately notify the CSE and appropriate regulator upon discovering a cybersecurity incident.

Second, companies should plan to review and update their incident response plans and cybersecurity policies in accordance with Bill C-8's reforms. Current and upcoming reviews should consider third-party and supply chain risks, including those posed by critical service providers (particularly those providing IT services), key suppliers, and device or product manufacturers. Once more information is provided, companies will also want to explore the extent to which their "critical cyber systems" can be segregated from other systems and whether doing so would assist in streamlining compliance efforts.

Third, companies subject to Bill C-8's reforms should consider how these new requirements could or should be reflected when contracting for services with third parties. Likewise, service providers should expect increasing cybersecurity standards from regulated customers, particularly when such services relate to critical cyber systems.

To discuss these issues, please contact the author(s).