Bill C-26: New Canadian critical infrastructure cyber security law

June 20, 2022

Canada has introduced a new cyber security law that will impose obligations on organizations acting in industries of national importance. The obligations will include mandatory cyber security programs and cyber incident reporting, and will be backed by administrative monetary penalties for non-compliance.

Overview

On June 14, the House of Commons introduced Bill C-26, which includes the newly drafted *Critical Cyber Systems Protection Act* (CCSPA) or in French, the *Loi sur la protection des cybersystèmes essentiels* (LPCSE). The CCSPA has been designed to "address longstanding gaps"[1] in the federal government's ability to protect systems and services of national importance and establishes a broad regulatory framework enabling the federal government to:

- define and strengthen baseline cyber security for systems and services of critical national importance;
- require certain organizations to develop and implement certain cyber security programs (CSPs);
- ensure that cyber incidents impacting vital systems and services are reported;
- issue binding Cyber Security Directions (CSDs); and
- encourage compliance through the introduction of administrative monetary penalties (AMPs).

We discuss each of these in greater detail below.

Impacted sectors

The CCSPA will impose duties on "designated operators" – operators that the government will designate by class and that are "persons, partnerships or unincorporated organizations that operate a work or carry on an undertaking or business [that is within the legislative authority of Parliament] in respect of a vital service or vital system".

Schedule 1 of the CCSPA identifies the specific vital services and systems that will be the basis of the designations:[2]

- telecommunications services;
- interprovincial or international pipelines and power line systems;
- nuclear energy systems;
- transportation systems within the legislative authority of Parliament;
- banking systems; and
- clearing and settlement systems.

Government will have the ability to add additional services and systems to the Schedule.[3] In other words, other federally regulated industries could be added to the Schedule, and consequently become subject to the CCSPA's requirements.

Each class of designated operators will be assigned a corresponding regulator – either the Minister of Industry, Minister of Transport, the Superintendent of Financial Institutions, the Bank of Canada, the Canadian Energy Regulator or the Canadian Nuclear Safety Commission.

Cyber security programs (CSPs)

Designated operators will be required to establish a cyber security program in respect of the critical cyber security systems they manage. A CSP must set out "reasonable steps" to:[4]

- identify and manage organizational cyber security risks, including risks relating to the operator's supply chain and use of third-party products and services;
- protect critical cyber systems from being compromised;
- detect cyber security incidents affecting critical systems; and
- minimize the impact of any cyber security incidents.

Designated operators will have an express duty to take reasonable steps to mitigate identified risks relating to their supply chains and use of third-party products and services.[5]

CSP filing and material change notification

Designated operators will be required to file CSPs with their regulator, to annually review their CSPs and to notify their regulator whether or not any amendments arose from review.[6]

They will also be required to notify their regulators of certain material changes, including (i) any material change in the designated operator's ownership or control and (ii) any material change in the designated operator's supply chain or in its use of third-party products and services.

Cyber Security Directions (CSDs)

The CCSPA provides for the issuance of CSDs – orders requiring operators or classes of operators to comply with measures to protect the cyber security of critical cyber systems. These directions may require designated operators to take specific actions in response to emerging cyber threats and other developments. The CCSPA also authorizes information sharing between government, regulators and law enforcement for any purpose related to the making, amending or revoking of a cyber security direction in respect of a designated operator[7].

Mandatory incident reporting

A key objective of the CCSPA is to preserve the continuity of vital services and systems by ensuring systems are not compromised, and to the extent that they are, that the compromise is detected and its impact minimized.[8]

As a result, the CCSPA requires designated operators to "immediately report a cyber security incident in respect of its critical systems" in accordance with the regulations[9]. The operator must report the incident to the Communications Security Establishment,[10] and must also immediately report the incident to their regulator.[11]

A "cyber security incident" is any incident which interferes or may interfere with (a) the continuity or security of a vital service or system, or (b) the confidentiality, integrity or availability of the critical cyber system.[12]

For those familiar with privacy breach reporting, cyber incident reporting under the CCSPA will be very different. Reporting is based on interference with critical systems or services, not to the information contained in systems or records. Reporting is also required based on the mere potential for interference, a matter of risk and probability that (under the current terms of the CCSPA) will be left to the interpretation of regulators and courts.

Record keeping

Designated operators will be required to keep records respecting cyber security incidents and other documents. The information that must be retained under the CCSPA will include:[13]

- any steps taken to implement the designated operator's cyber security program;
- every cyber security incident that the designated operator reported under section 17;
- any steps taken by the designated operator under section 15 to mitigate any supply-chain or third-party risks;
- any measures taken by the designated operator to implement a cyber security direction; and
- any other matter prescribed by the regulations.

Designated operators will be required to keep records in Canada at a place prescribed by regulation or, if no place is prescribed, at their place of business. They will also be required to keep records in the manner and for the period determined by the appropriate regulator unless another manner or period is prescribed by regulation.

Administrative monetary penalties (AMPs)

The CCSPA will allow each regulator to issue AMPs, with maximum penalties to be established by regulation at amounts of up to $15,000,000. An AMP may be issued for any violation of the CCSPA, including failing to report a cyber security incident and failing to comply with a CSD.[14]

Regulators will also have the authority to initiate regulatory proceedings leading to fines and possible imprisonment for non-compliance with the provisions of the CCSPA.

Conclusion

The CCSPA is a major development in Canadian cyber security law. Organizations who provide and operate the vital services and systems to which the CCSPA will apply may already have mature cyber security programs, but if the CCSPA passes they will face new requirements along with filing and reporting obligations. Filing and reporting is itself key component of the new Act, and is aligned with the type of government policy that many say is essential to combatting cyber crime. In this sense the CCSPA could benefit all organizations and citizens alike.

For more information on the CCSPA or any other assistance related to cyber security governance and response, please contact a member of our cyber security team.

Footnotes

[1] Protecting Critical Cyber Systems - Canada.ca

[2] CCSPA at Schedule 1.

[3] CCSPA at Section 6.

[4] CCSPA at Section 9(1).

[5] CCSPA at Section 15.

[6] CCSPA at Section 13.

[7] CCSPA at Section 23.

[8] CCSPA at Section 5.

[9] CCSPA at Section 17.

[10] Ibid and supra note 1.

[11] CCSPA at Section 18.

[12] CCSPA at Section 2.

[13] CCSPA at Section 30.

[14] See the sections on regulatory powers, beginning at CCSPA Section 32.

By

Shane Morganstein, Daniel J. Michaluk

Expertise

Cybersecurity, Privacy & Data Protection

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 725 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