FEDERAL GOVERNMENT PROPOSES NEW ACT TO REINFORCE CRITICAL CYBER SECURITY IN CANADA

Posted on July 5, 2022

Categories: Insights, Publications

On June 14, 2022, the federal government completed the first reading of Bill C-26, *An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts* (the "**Bill**").[1] The Bill would amend the *Telecommunications Act*[2] and enact the *Critical Cyber Systems Protection Act* ("**CCSPA**"), which would provide a framework for the protection of critical cyber systems of vital infrastructure in Canada. The stated purpose of the Bill is to help protect critical cyber systems in order to support the continuity and security of Canada's vital services and vital systems (which include its finance, energy, transportation and telecommunications sectors).

The Bill would do two main things: (1) amend the *Telecommunications Act* and (2) enact the CCSPA.

Amendments to the *Telecommunications Act*

The amendments to the *Telecommunications Act* would add a new objective to the Canadian Telecommunications Policy: the promotion of the security of the Canadian telecommunications system.[3] To further this objective, the amendments empower the Governor in Council and Minister of Industry to order a telecommunications service provider ("**TSP**") to do anything or refrain from doing anything that is necessary to secure the Canadian telecommunications system.[4] The Bill would also establish an administrative monetary penalty scheme to promote compliance with these orders and regulations as well as rules for judicial review. Administrative monetary penalties provided by the amendments would be as high as $25,000 for an individual ($50,000 for subsequent offense), or $10 million for any other entity ($15 million for subsequent offense).[5]

The Bill provides the government with significant powers to control TSPs when alleged to be necessary to protect Canada's national security. However, the Bill specifically provides that no one is entitled to any compensation for financial losses resulting from orders made under the above sections.[6]

These amendments follow the federal government's announcement that they would ban Huawei and ZTE from participating in 5G networks, and require companies to remove or terminate any existing 4G equipment provided by the companies by the end of 2027.

The Enactment of the CCSPA

The CCSPA would, among other things:

1. create new obligations for designated operators managing vital services or systems, including requirements to:
    - establish a cyber security program in accordance with regulations;[7]
    - take any steps to mitigate supply-chain risks identified by the cyber security program;[8]
    - immediately report any cyber security incidents in respect of critical cyber security systems to the Communications Security Establishment, and notify the appropriate regulator of the incident;[9]
    - comply with cyber security directions imposed by the Governor in Council;[10] and
    - Maintain certain records in accordance with regulations;[11]
2. empower the Governor in Council to direct designated operators to comply with any measure for the purpose of protecting a critical cyber system;[12]
3. allow for the exchange of information between various government entities for purposes related to a cyber security direction;[13]
4. prohibit the unauthorized disclosures of sensitive confidential information in respect of a critical cyber system;[14] and
5. provide certain regulators (including the Office of the Superintendent of Financial Institutions (OSFI), the Minister of Industry, the Bank of Canada, the Canadian Nuclear Safety Commission, the Canadian Energy Regulator, and the Minister of Transport) with the ability to investigate, make orders, and issue significant penalties for non-compliance (up to $1 million for individuals or $15 million in any other case).[15]

Currently, Schedule 1 of the bill lists the following as vital services and vital systems that would be subject to this framework:

- 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.

The designated operators to which the CCSPA would apply have not yet been specified.

We will continue to monitor these developments and provide further information when it is made available.

[1][ps2id id='1' target='/] Full text of the first reading available here.

[2][ps2id id='2' target='/] *Telecommunications Act*, SC 1993, c 38.
[3][ps2id id='3' target='/] *Telecommunications Act*, section 7 (j), as amended the Bill, section 1.
[4][ps2id id='4' target='/] *Telecommunications Act*, section 15.1 (1) and 15.2 (1) and (2), as amended the Bill, section 2.
[5][ps2id id='5' target='/] *Telecommunications Act*, section 72.131, as amended the Bill, section 7.
[6][ps2id id='6' target='/] *Telecommunications Act*, section 15.1 (6) and 15.2 (7), as amended the Bill, section 2.
[7][ps2id id='7' target='/] *Critical Cyber Systems Protection Act*, section 9(1), as enacted by the Bill, section 13.
[**CCSPA**]
[8][ps2id id='8' target='/] CCSPA, section 15.
[9][ps2id id='9' target='/] CCSPA, section 17 – 19.
[10][ps2id id='10' target='/] CCSPA, section 20.
[11][ps2id id='11' target='/] CCSPA, section 30.
[12][ps2id id='12' target='/] CCSPA, section 20.
[13][ps2id id='13' target='/] CCSPA, section 23.
[14][ps2id id='14' target='/] CCSPA, section 26.
[15][ps2id id='15' target='/] CCSPA, sections 32-85; 88-134.

by Robbie Grant

A Cautionary Note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.