SHIBLEY RIGHTON LLP
Barristers and Solicitors

Bill C-26 Introduces New Cybersecurity Requirements For Federally Regulated Industries

By Peter Murphy, Partner
Shibley Righton LLP
June 22, 2022

On June 14, 2022, Bill C-26 was introduced into the House of Commons of Canada. Bill C-26 proposes to enact the *Critical Cyber Systems Protection Act* (CCSPA), among other things, which would make certain federally-regulated private-sector organizations subject to new legal requirements regarding their cyber infrastructure.

The CCSPA's purpose is to "protect critical cyber systems in order to support the continuity and security of vital services and vital systems". If enacted, it will apply to designated operators that own, control or operate critical cyber systems.

A cyber system is considered "critical" where a compromise of the cyber system's confidentiality, integrity or availability could affect the continuity or security of a vital service or a vital system.

"Vital services and vital systems" are listed in Schedule 1 of the CCPSA, which currently include:

- nuclear energy systems;
- interprovincial or international pipeline or power line systems;
- telecommunications systems;
- federally-regulated transportation systems;
- banking systems; and
- clearing and settlement systems.

"Designated operators" will be listed in Schedule 2 of the CCSPA, by order of the Governor in Council. Designated operators will be required to establish and maintain a cybersecurity plan that sets out the designated operator's reasonable steps to do the following:

- identify and manage risks to its critical cyber system, including risks associated with the designated operator's supply chain and its use of third-party products and services;
- protect its critical cyber systems from being compromised;
- detect any cybersecurity incidents affecting, or having the potential to affect, its critical cyber systems;
- minimize the impact of cybersecurity incidents affecting its critical cyber systems; and
- do anything else that is prescribed by the regulations.

In addition, designated operators will be required to:

- conduct cybersecurity program annual reviews;
- mitigate cybersecurity threats arising from the supply chain or from third party products or services;
- share their cybersecurity programs with the appropriate regulators;
- report cybersecurity incidents to the Canadian Security Establishment;
- comply with cybersecurity directions from the Governor-in-Council; and
- maintain related records.

The CCSPA will apply regardless of whether personal information is involved. As a result, the CCSPA will impose cyber security requirements on subject organizations separately from the requirements of Canadian private sector privacy law, in a manner that is similar to the *Office of the Superintendent of Financial Institutions'* cybersecurity guidelines that currently apply to Canada's federally regulated financial institutions.

The CCPSA contains significant enforcement provisions. Regulators of designated operators will be given investigatory, auditing and order-making powers, including the ability to enter into compliance agreements. They will also be empowered to issue administrative monetary penalties of up to $1,000,000 per day for individuals and up to $15,000,000 per day for organizations. In addition, the Federal Court will be given jurisdiction to issue fines against, or order the imprisonment of, designated operators and their directors and officers.