MARCH 2018

CYBERSECURITY BULLETIN

Borden Ladner Gervais

Cybersecurity Framework for Ontario's Electricity Industry

On March 15, 2018, the Ontario Energy Board ("OEB") issued a Notice of Amendments to the Ontario Transmission System Code and Distribution System Code to require licensed electricity transmitters and distributors in Ontario to use an industry-developed Ontario Cyber Security Framework to provide the OEB with information about their cybersecurity and privacy maturity. The Framework's integration of cybersecurity and privacy controls may be useful to organizations in other industries.

Cybersecurity and the Framework

The code amendments define "cyber security" as "a body of technologies, processes, and practices designed to protect networks, computers, programs, data and personal information from attack, damage or unauthorized access", and reference both electronic and physical security. The code amendments require each licensed electricity transmitter or distributor to use the Ontario Cyber Security Framework to report on their cyber security readiness.

The Framework is comprised of an Inherent Risk Profile Tool and a related Self-Assessment Questionnaire, which are mapped to cybersecurity controls and privacy controls. The cybersecurity controls are based on the U.S. National Institute of Standards and Technology ("NIST") *Framework for Improving Critical Infrastructure Cybersecurity*, which has been widely adopted and endorsed as a foundational cybersecurity resource by regulators and industry associations around the world, including in Canada. The privacy controls reflect *Fair Information Principles* (which are the foundation of Canadian personal information protection laws) and *Generally Accepted Privacy Principles* (established by the American Institute of Certified Public Accountants and Chartered Professional Accountants Canada). The Framework can be used to assess an organization's inherent cybersecurity and privacy risks, define an organization's benchmark objectives and measure an organization's progress toward those objectives.

Licensed transmitters and distributors are required to report their cybersecurity maturity and provide a self-certification (signed by the chief executive officer) to the OEB on an annual basis. The first interim report is required by June 15, 2018, and annual self-certifications are required starting April 30, 2019. The OEM will establish requirements for reporting and self-certifications.

The Privacy Controls

The Framework explains: "Integrating privacy with the NIST controls is an innovative approach that provides a complete perspective on cyber security and privacy". The added privacy controls are as follows:

- The organization is able to identify: the personal information or customer proprietary information in its custody or control; its authority for the collection, use and disclosure of such information; and the sensitivity of such information.
- Responsibility for the privacy management program has been established.
- Senior management is committed to a privacy-respectful culture.
- A policy is established for collection, use and disclosure of customer personal and proprietary information, including requirements for consent and notification.
- A policy is established for retention and disposal of customer personal or proprietary information.
- Governance and risk management processes address privacy risks.
- Activities and processes that involve the collection, use or disclosure of personal or customer proprietary information are identified.
- Privacy impacts are considered when a new process, technology or activity is contemplated.
- Documentation is developed to explain the organization's personal information policies and procedures to staff and customers.
- Privacy is included in human resources practices (e.g. privacy training).
- Policies for receiving and responding to privacy complaints or inquiries are established and communicated to customers.

Information Sharing and Additional Activities

The Notice of Amendments explains that the OEB expects the electricity sector to collaborate and actively share experiences, knowledge and information to enhance efficiency and efficacy in responding to cybersecurity threats, including by establishing a structured information sharing process (i.e. a Cyber Security Information Sharing Forum). The Notice of Amendments also explains that the OEB expects the Framework to continue to evolve, under the guidance of a Cyber Security Advisory Committee, to provide guidance to licensed transmitters and distributors to support their cybersecurity maturation.

Comment

The OEB's code amendments and Framework are consistent with cybersecurity and privacy guidance issued by privacy commissioners, regulators and self-regulatory organizations, and with information security practices detailed in regulatory reports and data breach lawsuit settlements. The Framework will assist licensed electricity transmitters and distributors to assess their personal information practices and cybersecurity readiness against industry recommended best practices. While the Framework has some elements designed specifically for the electricity industry, the Framework may be useful for organizations in other industries.

For more information regarding cybersecurity and privacy law compliance, see BLG bulletins: *Regulatory Enforcement Action Emphasizes Need for an Information Security Governance Framework*; *Cybersecurity Guidance from Canadian Securities Administrators*; *Cyber Risk Management Guidance for Corporate Directors*; *G7 Cybersecurity Guidelines for the Financial Sector*; *G-7 Guidelines for Cybersecurity Assessment*; *VTech Data Breach Enforcement Actions – Guidance for Data Security and Privacy Law Compliance*; *Settlement of Uber Privacy/Data Security Complaint – Cybersecurity Guidance*; *Settlement of Walmart Canada Photo Centre Data Breach Lawsuits – Lessons Learned*.

For more information on OEB regulatory developments, see BLG bulletins: *Proposed Regulation to Require All Ontario Utilities to Implement Green Button by July 1, 2020*; *Ontario Energy Board Issues Final Report on the Regulatory Treatment of Costs Associated with Pension and Other Post-Employment Benefits*; *Ontario Net Metering Regulation: Ministry Posts Updated Regulatory Proposal*; *OEB Staff Confirm That Electric Vehicle Charging Stations Can Be Owned and Operated by LDCs*; *The OEB's New Consumer Engagement Framework*; *Summary of Proposed Amendments to the Ontario Energy Board Act, 1998*. ■

Authors

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

John Vellone
T 416.367.6730
jvellone@blg.com

BLG's Cybersecurity Law Group assists clients with legal advice to help manage cyber risks and to respond to data security incidents. Information about BLG's Cybersecurity Law Group is available at blg.com/cybersecurity.

BLG's Electricity Markets Group is a multidisciplinary team that has the expertise to advise on legal and business issues, opportunities and developments facing the electricity sector. More information is available at http://blg.com/en/Expertise/ElectricityMarkets.

BLG Cybersecurity Group – Key Contacts

Bradley J. Freedman	Vancouver	604.640.4129
Éloïse Gratton	Montréal	514.954.3106
Kevin L. LaRoche	Ottawa	613.787.3516
David Madsen	Calgary	403.232.9612
Ira Nishisato	Toronto	416.367.6349

BLG Vancouver
1200 Waterfront Centre, 200 Burrard St
Vancouver, BC, Canada V7X 1T2
T 604.687.5744 | F 604.687.1415
blg.com