Ontario Cyber Security Standard: Impact on licensed electricity transmitters and distributors

November 29, 2024

On Oct. 1, 2024, amendments to the Ontario Energy Board's (OEB) *Transmission System Code* (TSC) and *Distribution System Code* (DSC, and together, the Codes) came into force. The amendments are intended to facilitate and enhance cyber security readiness, collaboration and innovation in Ontario's electricity sector.

The amendments require licensed electricity transmitters and distributors (utilities) to comply with the new Ontario Cyber Security Standard (the Standard), which lays out cyber security readiness requirements.

The legal implications of this change are significant. Contravention of a condition of a transmission or distribution licence constitutes contravention of an "enforceable provision" under the *Ontario Energy Board Act, 1998* (the OEB Act), which itself gives rise to a range of enforcement powers held by the OEB under Part VII of the OEB Act to make inquiries, appoint inspectors and conduct inspections, appoint investigators and conduct investigations, and a range of powers to remedy the non-compliance including issuing orders that a party must remedy a contravention that has occurred, or prevent a contravention or further contravention from occurring; suspending or revoking the distribution or transmission licence, as applicable, and requiring the person to pay administrative monetary penalty not to exceed $1,000,000 for each day or part of a day on which the contravention occurs or continues.

For further background, please see BLG's previous article on the Cybersecurity Framework for Ontario's Electricity Industry, which covers a prior Notice of Amendments (from March 15, 2018) that required licensed electricity transmitters (under the TSC) and distributors (under the DSC) to comply with the Ontario Cyber Security Framework (the Framework and report information about their cyber security and privacy maturity to the OEB.

Enacted amendments

To be specific, the OEB has enacted mirroring amendments in each of the Codes that:

1. Add the definition of "Cyber Security Standard", which means "the Cyber Security Standard Document issued on March 27, 2024, as updated from time to time."[1]

2. Add a section called “Compliance with the Cyber Security Standard,” which requires the transmitter (in the case of the TSC) or the distributor (in the case of the DSC) to comply with the Cyber Security Standard.[2]

The Ontario Cyber Security Standard

The Standard’s purpose is to “enhance the cyber security readiness of Ontario’s electricity system.” Perhaps the most significant benefit of the Standard is that it will enable the OEB to respond to changing industry standards or cyber security risks by quickly updating cyber security requirements. However, the Standard itself currently implements two essential requirements to increase the cyber security readiness of utilities, specifically:

1. **Utilities are required to participate** (and confirm such participation as required by the OEB) in the Independent Electricity System Operator’s (the IESO) Lighthouse service;[3] and
2. **Applicable transmitters and distributors must implement specific control objectives** related to governance and privacy of the Framework and **subsequently report on the objectives’ implementation.** [4]

The IESO’s Lighthouse service (free of cost to Ontario utilities) aims to increase cyber security readiness through a threat information sharing process. This ensures all participating utilities have access to near real-time information and situational awareness services, as provided by the IESO (as mandated by the OEB).

As described on the IESO’s website, the IESO’s Lighthouse service provides “world-class analysis” through its partnership with the Canadian Centre for Cyber Security (the Cyber Centre) and through three key steps:

1. The IESO collects information from the utilities participating in the Lighthouse service, which it can then share with the Cyber Centre.
2. The Cyber Centre analyzes the information provided by IESO using cyber defence tools and conducts a “continuous and comprehensive assessment of cyber risks.”
3. The IESO provides cybersecurity products and reports to participating utilities, providing insights into threats and situations that may impact the participants themselves and the sector more broadly.

The types of reports that the IESO provides to utilities through its Lighthouse service include:

1. **Flash advisories** : focused on enhancing situational awareness);
2. **Tactical threat intelligence reports** : focused on threats and vulnerabilities from a technical perspective); and
3. **Strategic threat intelligence reports** : geared towards management and provide information on important trends).

The portions of the Framework that the Standard mandates utilities to implement and subsequently report on, per the OEB’s Notice of Proposal, “call for utilities to develop

cyber security policies, roles and responsibilities, and processes to aid the identification, assessment, and management of cyber security risks."

The Standard lists the control objectives utilities must implement (and report on their implementation) in section 4. Section 4.1 mandates that a transmitter or distributor implement the following control objectives of the Framework at a Maturity Indicator Level two:

a. **ID.AM-6** (cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established);
b. **ID.GV-1** (organizational cybersecurity policy is established and communicated), **2** (cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners), **3** (legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed), and **4** (governance and risk management processes address cybersecurity risks);
c. **PR.AT-4** (senior executives understand their roles and responsibilities) and **5** (physical and cybersecurity personnel understand their roles and responsibilities); and
d. **ID.RM-1** (risk management processes are established, managed, and agreed to by organizational stakeholders).

Section 4.2 mandates that a transmitter or distributor implement the following control objectives of the Framework:

a. **ID.AM-P1** (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), and **2** (responsibility for the privacy management program has been established);
b. **ID.GV-P1** (a policy is established for collection, use and disclosure of customer personal and proprietary information, including requirements for consent and notification), **P2** (a policy is established for retention and disposal of customer personal or proprietary information), and **P3** (governance and risk management processes address privacy risks);
c. **ID.RA-P1** (activities and processes which involve the collection, use or disclosure of personal or customer proprietary information are identified); and
d. **ID.RM-P1** (privacy impacts are considered when a new process, technology or activity is contemplated).

Compliance, costs and benefits

Compliance with the Standard (and the amended Codes) will be monitored through the annual cyber security reports that all transmitters and distributors must submit to the OEB (each April) per the OEB's *Reporting and Record Keeping Requirements*.

Both the anticipated costs and benefits of the amendments were discussed in the OEB's Notice of Proposal. The OEB expects the implementation of the Standard's first requirement to be low-cost, given that the Lighthouse Service is free. However, in some cases, a capital investment may be required to ensure a utility can establish a secure network connection with the Lighthouse service's infrastructure. Implementation of the

Standard's second requirement is also expected to be low-cost, given the governance and privacy-related requirements primarily consist of policies, processes, and structures.

In summary, the OEB takes the position that any costs transmitters or distributors incur will be well worth the benefit the Standard will bring through the utilities' mandatory participation in the IESO's Lighthouse service and implementation of the relevant governance and privacy control objectives.

Key takeaway

The amendments to the Codes give effect to the Standard, enabling the OEB to address cyber security risks and other urgent developments faster. This is a welcome and timely development in a rapidly developing industry facing potential severe cyber security threats.

Given the minimal (if any) capital investment requirements, the Standard should also be seen as a benefit to utilities. Given mandatory participation, having access to the Lighthouse service will provide transmitters and distributors not only with control objectives that help ensure their data, information and organizational decision-making are protected but, more importantly, with access to critical information, tools, and other products that will increase their ability to respond to the cyber security threats that they and the broader sector face.

To learn more about cyber security and privacy law compliance, explore BLG Insights:

- New outsourcing guidance by Ontario public sector privacy regulator
- What you need to know about the new Regulation respecting the anonymization of personal information
- LifeLabs: Court considers privilege claims over cybersecurity investigation materials
- *Bill 194 - The new Enhancing Digital Security and Trust Act, 2024 and changes to* Ontario's *Freedom of Information and Protection of Privacy Act*
- Lucky 7 data privacy and security cheat sheet
- 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 insights from our Energy team on OEB regulatory developments, explore BLG Insights:

- Proposed changes to Ontario's leave to construct requirements

- OEB's latest guidance on distributed energy resources connections
- OEB Issues Corporate Governance "Best Practices" for Rate-Regulated Utilities
- 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

To learn more about how the above amendments affect your organization, please get in touch with any of the contacts below.

Footnotes

[1] The definition has been added to section 3B.2.1 of the TSC and 1.2 of the DSC.

[2] This amended section is found in section 3B.2.4 of the TSC and 6.8.3 of the DSC.

[3] As outlined in section 3 of the Standard.

[4] As outlined in section 4 of the Standard.

By

Daniel J. Michaluk, Kristyn Annis, John A.D. Vellone, Nicholas Pinsent

Expertise

Cybersecurity, Privacy & Data Protection, Energy – Power, Technology

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