Electricity Canada Submission

Bill C-26

Part 2 – Critical Cyber Systems Protection Act

May 2023

613.230.9263
info@electricity.ca
electricity.ca | **electricite.ca**

1500-275 Slater Street
1500-275, rue Slater
Ottawa, Ontario K1P 5H9

LIST OF RECOMMENDATIONS

North American Regulatory Alignment

- Include provisions allowing the *regulator* to release a designated operator from the obligation to develop a cyber security program.
- Encourage the *Governor in Council* to align relevant definitions, including the definition of cyber security incident, with NERC's definitions.
- Include provisions allowing the *Governor in Council* to take measures and establish mechanisms to avoid duplication or overlap with jurisdictions attributed to provincial regulatory agencies.
- Ensure that a *designated operator* cannot be subject to a double penalty in systems that may have more than one regulator.

Reporting

- Include provisions allowing the *Governor in Council* to take measures and establish mechanisms to harmonize the reporting process with existing cyber security incident reporting processes.
- Remove references to compliance periods.
- Include provisions granting legal protection to operators regarding information shared with the Communications Security Establishment pursuant to this Act.
- Amend s. 14 (1) (b) and remove excessive reporting requirements on supply chain and use of third-party products and services.

Protecting Existing Collaboration

- Exempt the Canadian Centre for Cyber Security from obligations to report information obtained by way of this Act to other entities.
- Amend the sections on "Disclosure and Use of Information" to permit the exchange of information with NERC.
- Amend s 25 (1) to allow *designated operators* to disclose to trusted industry partners that a direction was issued.

Transparency

- Include an obligation for the Minister to annually report the number of cyber security directions issued as well as the compliance rate to those orders.
- Include provisions that lift the prohibition against disclosure of cyber security directions after a reasonable amount of time.

Regulation Making Process

- Leverage and seek input from existing critical infrastructure forums during the regulation-making process.

About Electricity Canada

Electricity Canada is the national voice of Canada's evolving and innovative electricity business. Our members generate, transmit, and distribute electrical energy to industrial, commercial, residential, and institutional customers across Canada. Members include integrated electric utilities, independent power producers, transmission and distribution companies, power marketers, and system operators, who deliver electricity to all Canadians in every province and territory.

Cyber security and the electricity sector

The cyber threat to the Canadian electricity industry has been increasing year-over-year, with increases in both the number and sophistication of attacks. Canadian electricity companies have a long track record of working to protect their critical assets against emerging threats, and have been collaborating with each other and with government partners on cyber security issues for over two decades.

Indeed, the sector often engages in information-sharing and best practice development for a diverse set of security-related issues affecting the electricity industry, and works in partnership with security and intelligence officials and policymakers in Canada and abroad.

The sector has successfully established relationships with government partners such as the Canadian Centre for Cyber Security, Natural Resources Canada, and Public Safety Canada. It also regularly interfaces with international partners, including the U.S. Department of Energy (DOE), the North American Electric Reliability Corporation (NERC), the Federal Energy Regulatory Commission (FERC), the Electricity Information Sharing and Analysis Center (E-ISAC) and the provincial regulators. These partnerships ensure access to information and tools to help the industry secure its critical systems.

Electricity Canada recommendations for the *Critical Cyber Systems Protection Act*

Overview

Electricity Canada supports measures that strengthen the overall security posture of the country and of the electricity sector. Governments and industry have a joint responsibility to ensure our critical infrastructure is well protected against threats, and collaboration between the two is key.

However, collaboration is built on trust and dependent on the mutually beneficial exchange of information. While mandatory security requirements can help strengthen our overall security posture, the approach taken by Bill C-26 risks having the opposite effect. It does not recognize established security standards and expertise within our sector. In practice, the bill risks adding very little security to our sector, and redundantly adds an additional layer of regulatory requirements.

It is important that Bill C-26 does not create unintended barriers to collaboration and ensures that new measures are aligned with the existing regulatory framework. It should provide tools and protocols to add to the safety of Canada's critical infrastructure sector.

North American Regulatory Alignment

One of our key concerns with Bill C-26 is the risk of creating dual and potentially competing regulatory systems. More specifically, the bill has the potential to regulate areas that are generally already covered by existing requirements found in NERC Critical Infrastructure Protection CIP standards, which have been adopted, enforced, and audited by many provincial regulators[1]. Moreover, the bill seems to extend the regulators' jurisdiction to provincial areas of responsibility.

Overall, this risks creating conflict between different regulators, enhancing the regulatory burden for operators, causing confusion and ambiguity on compliance, and ultimately hindering the goal of Bill C-26, which is to make our critical systems safer.

Ensuring that measures coming out of the bill are aligned with the current North American regulatory framework and do not compete with provincial regulators should therefore be a priority.

Recommendation: Include provisions allowing the regulator to release a designated operator from the obligation to develop a cyber security program.

Under the Act, the *regulator* does not have the power to release a *designated operator* from the obligation to develop a cyber security program or modify its terms or conditions if appropriate standards already exist. A provision to this effect could be added to the Act.

NERC Reliability Standards are highly regarded within the electricity community, both by the industry and provincial regulators. They are developed using an industry-driven process that ensures it is open to all persons who are directly and materially affected by the reliability of the North American bulk power system; transparent to the public; demonstrates the consensus for each standard; fairly balances the interests of all stakeholders; provides for reasonable notice and opportunity for comment; and enables the development of standards in a timely manner.

The NERC CIP standards are the mandatory security standards that apply to most entities that own or manage facilities that are part of the U.S. and Canadian electric power grid. Indeed, the standards are mandatory and enforceable in almost all provinces connected to the bulk electric system (BES). They require utility companies in North America to establish and adhere to a baseline set of cybersecurity measures.

Given our sector's mature cyber security posture and the existing North American cyber security standards, the *regulator* should be able to determine if existing measures are sufficient to meet the

[1] For ease of reading "NERC CIP" is hereinafter used throughout out the document to refer to NERC CIP standards as well as to the NERC CIP standards under the authority of provincial regulatory bodies.

requirement under the Act and release a *designated operator* from its obligations. This would be an easy fix to avoid duplication of efforts and regulatory burden.

Recommendation: Encourage the Governor in Council to align relevant definitions, including the definition of cyber security incident, with NERC's definitions.

The regulations that are to be developed after the passage of the bill are likely to introduce definitions that differ from the existing regulatory regime. This may cause unnecessary confusion and ambiguity for operators.

For example, definitions of what constitutes a critical cyber system or a cyber security incident are likely to be different from the ones already used in NERC CIP standards. These new definitions could extend the range of cyber security incidents that operators usually have to report.

Therefore, the bill should include provisions encouraging the *Governor in Council* to align relevant definitions with definitions already developed by NERC.

Recommendation: Include provisions allowing the Governor in Council to take measures and establish mechanisms to avoid duplication or overlap with jurisdictions attributed to provincial regulatory agencies.

The *Canadian Energy Regulator Act* (CERA) states that provincial laws apply to the intraprovincial sections of an international transmission line, and that a province can designate a regulatory agency to exercise its powers, rights and privileges over those sections.

With regard to interprovincial lines, CERA provides that in order to fall under the jurisdiction of the Canadian Energy Regulator (CER), an interprovincial line must be designated by order as a line whose construction and operation require the issuance of a certificate. The CER website mentions that no interprovincial line has received such designation to date. Therefore, no interprovincial line is currently subject to the jurisdiction of the CER.

Bill C-26 includes interprovincial and international power line systems as *vital systems*, and thus subject to the Act. It also identifies the CER as the *regulator* of this vital system.

Given the above, Bill C-26 appears to expand the CER's jurisdiction over areas that are currently under provincial jurisdiction. As is the case for sections 253 and 254 of CERA, Bill C-26 makes no distinction between the intraprovincial and international sections of an international line. Therefore, in the area of cyber security, and in accordance with Bill C-26, the CER's jurisdiction would cover the entire international line, including its intraprovincial sections, which are currently subject to provincial laws and the jurisdiction of the provincially designated regulatory agency.

In addition, while no interprovincial line has been designated by an order of the federal government under the CERA, the Act could apply to such a line in the absence of a designation. Schedule 1 to Bill

C-26 makes no distinction in this regard. In the area of cyber security, all interprovincial lines would fall under the jurisdiction of the CER, including lines that have not been designated.

To avoid competing regulatory systems, further clarity must be provided within the Act. This could be done by recognizing, within the Act, the application of provincial laws and the jurisdiction of the province's regulatory agency over undesignated interprovincial lines and over the intraprovincial section of an international transmission line. It must also include provisions allowing the *Governor in Council* to take measures and establish mechanisms to avoid duplication or overlapping with other jurisdictions.

Recommendation: Ensure that a designated operator cannot be subject to a double penalty in systems that may have more than one regulator.

Provincial regulators have the power to issue sanctions and penalties for violations of a reliability standard requirement. Because Bill C-26 would regulate areas generally already covered by existing NERC CIP requirements, an operator may be unfairly subject to a double penalty in case of a violation. The bill should include provisions that remove the possibility of a double penalty in systems that may have more than one regulator.

Reporting

The mandatory reporting of cyber security incidents is a significant part of Bill C-26. It's also a significant break from current practice, where operators' reporting of incidents to federal authorities is voluntary. While we understand the importance of the federal government being notified quickly and consistently of cyber security incidents, we see some important gaps in the bill. Amendments are needed to ensure reporting requirements are not duplicative or excessive, and to ensure operators do not open themselves to legal risks by complying with said requirements or by voluntarily sharing information with federal partners.

Recommendation: Include provisions allowing the Governor in Council to take measures and establish mechanisms to harmonize the reporting process with existing cyber security incident reporting processes.

NERC-regulated entities are already subject to mandatory reporting of cyber security incidents. A reportable cyber security incident must be reported to the Electricity Information Sharing and Analysis Center (E-ISAC) within one hour of determining that an event is a reportable cyber security incident or by the end of the next calendar day after determining that a cyber security incident was an attempt to compromise a cyber system.

As stated previously, Bill C-26 provides a different definition of a cyber security incident than the one used in NERC CIP standards. This new definition could extend the range of cyber security incidents that must be reported to the CSE.

Harmonization of the reporting processes appears necessary because, in an emergency, the determination of whether a cyber security incident should be reported, whether to the E-ISAC or to the

CSE, must be made quickly and without excessive effort. Any confusion or ambiguity regarding the determination of cyber security incidents may result in delays that could jeopardize the grid.

Recommendation: Remove references to compliance periods.

Cyber security requirements, especially incident reporting requirements, should not distract critical infrastructure operators from their response and recovery efforts following an incident. Reporting requirements should be well-defined, consistent, and have a reporting timeline that is flexible enough to allow the effective use of limited resources during incident response and recovery.

The timeline for reporting cyber security incidents is also usually based on when an incident is determined to be reportable, and not on the time of the actual incident. Any reference to the timeline for reporting cyber security incidents should be left to the regulations. Therefore, the word "immediately" should be removed from s 17.

Similarly, the words "without delay" should also be removed from s. 14.

Recommendation: Include provisions granting legal protection to operators regarding information shared with the Communications Security Establishment pursuant to this Act.

Unless the bill includes provisions granting legal protection to critical infrastructure operators that report information to the CSE, operators will generally be reluctant to share additional information and to provide voluntary reports of incidents that may not fall within the scope of the regulations. As the Standing Committee on Public Safety and National Security heard during its *Assessment of Canada's Security Posture in Relation to Russia* last year, "safe harbour" provisions are an important part of promoting information-sharing between industry and government. Including provisions that reduce the legal risks of critical infrastructure operators will be very important to ensure the successful implementation of the new reporting requirements and the overall goals of the legislation.

Last year, the United States passed the *Cyber Incident Reporting for Critical Infrastructure Act 2022 (CIRCIA)*. The act includes provisions that provide liability protections to reporting entities. We recommend that similar language be included in Bill C-26. Those legal protections should also be extended to voluntary reports, as provided for in CIRCIA.

Recommendation: Amend s. 14 (1) (b) and remove excessive reporting requirements on supply chain and use of third-party products and services.

The bill requires the development of a cyber security program to manage risks associated with the designated operator's supply chain and use of third-party products and services. This program will require the development of a list of third-party products and services that, if compromised, may impact a vital service or a vital system. The cyber security program allows the ongoing management of supply chain risk as products and services are added and removed.

Under section 14 (1) (b) a designated operator must notify the regulator of any material change in the designated operator's supply chain or in its use of third-party products and services. We recommend that this provision be amended or replaced with a less onerous and more adapted provision.

Section 14 (1) (b) adds additional reporting requirements without an additional gain in cyber security. It has the potential to delay the process of purchasing and acquiring needed software and services, in a market environment where the supply chain is already strained. When considering all of the control systems that may impact a vital service, including central control centers, a great number of software programs might be in use over hundreds of computer systems. This makes the provision an arduous reporting exercise.

This provision also creates additional risks to the security of the vital system by creating a central list of third-party products and services that may impact vital systems should they be compromised. This list would then be shared and visible to parties that do not require this type of information.

Alternatively, we propose that the operator should be allowed to manage supply chain risk without reporting all of the software and services in use. Instead of requiring operators to notify the regulator of "material changes", records relating to the supply chain risk management process should stay with the designated operator and be available for review under provisions allowing the regulator to audit the designated operators' cyber security program. This would enable the regulator to verify the operators' supply chain risk management process, without adding excessive reporting requirements or creating additional security risks.

Protecting Existing Collaboration

As currently written, we fear that Bill C-26 may have unintended consequences on existing collaboration within the industry, as well as with governments and North American regulators. We urge the committee to consider these recommendations to ensure that existing collaboration, which helps keep our critical infrastructure secure, is not negatively impacted by this bill.

Recommendation: Exempt the Canadian Centre for Cyber Security from obligations to report information obtained by way of this Act to other entities.

Since the creation of the Canadian Centre for Cyber Security (Cyber Center) in 2018, industry and government have been able to collaborate more closely on cybersecurity issues. This has strengthened the overall security posture of the country. However, the collaboration between the industry and the Cyber Center is built on trust. Trust that information shared with the Cyber Center isn't shared with regulators or enforcement agencies. Bill C-26 puts this collaboration at risk.

To protect the existing and positive collaboration between critical infrastructure operators and the Cyber Center, we recommend that the bill isolates the Cyber Center from any information-sharing obligations provided for in the legislation.

While the roles of these organizations are different, the relationship between NERC, provincial regulators and the Electricity Information Sharing and Analysis Center (E-ISAC) is an example of how

an agency can earn the trust of critical infrastructure operators and encourage information sharing with them. While the E-ISAC is operated by NERC, it is organizationally isolated from NERC's enforcement processes. This means that the information that operators report to E-ISAC will not be shared with NERC.

Recommendation: Amend the sections on "Disclosure and Use of Information" to permit the exchange of information with NERC.

Restrictions exist within the bill as to the organizations with which federal authorities can enter into agreements or arrangements for the purpose of exchanging information – the government of a province or one of its institutions, a foreign state or an international organization established by the governments of various states. However, it is unclear whether NERC meets the definition of "international organization" given it is an international non-profit organization under the oversight of FERC.

NERC was not established by any government. Rather, it was established by an agreement on June 1, 1968, among 12 regional organizations managing US power systems and parts of systems in Ontario, British Columbia and Manitoba. The E-ISAC, which is operated by NERC but is distinct from an organizational standpoint, does not qualify as an international organization either. Therefore, federal authorities would not be allowed to enter into an agreement with NERC and the E-ISAC concerning the disclosure of information, whether or not the information is confidential.

Concerns would be justified regarding the potential for the co-existence of mechanisms established by the Act and those currently in place. The two mechanisms require the communication of information, much or most of which is confidential within the meaning of the Act. Although the disclosure of confidential information is permitted when required to protect vital systems and critical cyber systems (s 26 (1)(d)), it is not certain whether operators can continue to refer to NERC for cyber security issues and to report cyber security incidents to the E-ISAC.

In addition, unless an agreement or arrangement can be entered into between the federal authority and NERC, operators would not be authorized to directly disclose to NERC the existence of a direction and measures that the federal government orders it to take under this direction. It is important to recall that the content and existence of a direction constitute information that cannot be disclosed (ss 24 and 25).

We should add that, in the CIP standards as adopted (for example, CIP-008-5), the provincial regulators may refer to NERC standards as well as to the E-ISAC's mechanisms for reporting cyber security incidents. The *Régie de l'énergie du Québec*, for example, has also entered into an agreement concerning the Québec Reliability Standards and Compliance Monitoring and Enforcement Program (QCMEP) under which it retains the services of NERC and the NPCC to [translation] "monitor and assess compliance of entities subject to reliability standards in Québec" (Clause 3). Under this agreement, NERC and the NPCC can remotely access a data warehouse containing information that is not public.

To protect existing collaboration that makes our grid safer, the bill should be amended to permit the exchange of information with NERC or with any regional entity in which the provincial regulators have

entered an agreement. It should also ensure that any agreement or arrangement entered into between the federal authority and provincial regulators permits recognition of the agreement between them, NERC and the regional entities.

Recommendation: Amend s 25 (1) to allow designated operators to disclose to trusted industry partners that a direction was issued.

The electricity sector has a long history of providing mutual assistance to fellow utilities in times of need. The sector's security officials also regularly meet to discuss shared challenges, threats, and best practices. In times of crisis, maintaining the sector's ability to mobilize and ask for assistance when needed is critical.

The sector is currently facing significant labour and skills shortages in cyber security. Therefore, the sharing of expertise between critical infrastructure operators helps strengthen our sector's security posture.

S 25 (1) should be broadened to allow the disclosure of a cyber security direction for the purpose of receiving mutual assistance from trusted industry partners, and to protect the operators' collaboration with identified response partners.

The bill should also clarify the operators' ability to disclose *directions* to provincial partners, including provincial regulators. This is particularly important in cases where a direction may conflict with existing regulatory requirements. In such cases, operators unable to disclose that a direction was issued may fail audits by their provincial regulators.

Transparency

We understand that national security requires a certain level of secrecy. However, we believe that some provisions could be added to this bill to offer reasonable and practical levels of transparency.

Recommendation: Include an obligation for the Minister to annually report the number of cyber security directions issued as well as the compliance rate to those orders.

While s 146 requires the Minister to annually "prepare a report on the administration of this Act", it is not clear whether this obligation will provide sufficient levels of transparency. The committee should amend s 146 and add specific reporting requirements for the Minister. While it may be reasonable for government to withhold the content of cyber security directions from the public eye, the government should be transparent with Canadians on how often it uses the powers in the Act. Annual reporting on the number of cyber security directions issued as well as the compliance rate to those orders would be a step in the right direction, allowing the public and industry to better understand the extent to which the powers in the bill are being used.

Recommendation: Include provisions that lift the prohibition against disclosure of cyber security directions after a reasonable amount of time.

For further transparency, the bill should include provisions that lift the prohibition against disclosure after a reasonable amount of time. As currently written, it is possible that the prohibition against disclosure for all directives to never be lifted, which means Canadians and the industry will never realize the extent of the government's use of the new powers.

Short of a complete lifting of the prohibition against disclosures, provisions should allow government agencies and critical infrastructure operators to meet and discuss the content of security directions. This kind of information sharing would help operators identify common vulnerabilities and better defend their systems, strengthening the overall security posture of our sector.

Regulation Making Process

Bill C-26 is an enabling piece of legislation, with further details to be developed during the regulation-making process. Given the bill's significant impact on critical infrastructure operators, existing forums should be leveraged during the consultation process.

Recommendation: Leverage and seek input from existing critical infrastructure forums during the regulation-making process.

The critical infrastructure community is made up of experienced individuals with great knowledge of the security issues facing their sector. Critical infrastructure operators in the electricity sector are already engaged in existing regulatory rule-making processes through NERC. Leveraging that experience would not only help ensure that the new regulations do not unnecessarily duplicate existing measures, but also ensure they have a high and positive impact on the security posture of our country and our critical infrastructure.