Electricity Canada | Électricité Canada

Brief to Standing Committee on Public Safety and National Security

Bill C-8 – Critical Cyber Systems Protection Act

November 2025

Electricity Canada is the national voice of the electricity sector, representing companies that generate, transmit, and distribute electrical energy to residential, commercial, industrial and institutional customers in every province and territory.

Canadian electricity companies have a long track record of working to protect their critical assets against cyber threats and have been collaborating with government partners on cyber security issues for over two decades.

While Electricity Canada is supportive of the bill's overall objectives, including increasing the federal government's visibility over cyber-attacks on critical infrastructure and ensuring a consistent cross-sectoral approach to cyber security, we also offer feedback that we believe will allow Bill C-8 to strengthen partnerships with federal agencies and bolster our sector's security posture.

SUMMARY OF RECOMMENDATIONS

REGULATORY DUPLICATION

1. **Recognize Equivalent Regulatory Frameworks** – Include provisions that allow the regulator to acknowledge and accept compliance with equivalent frameworks. For example, electricity operators could fulfill Bill C-8's requirements for cybersecurity programs and supply chain risk management through their existing compliance with NERC CIP standards.

2. **Harmonize Incident Reporting Requirements –** Include provisions enabling the Governor in Council to establish mechanisms that align Bill C-8's incident reporting requirements with existing provincial and NERC CIP processes. Harmonization is essential to ensure timely and effective reporting, allowing operators to concentrate their efforts on incident response and recovery.

RISKS TO CYBER CENTRE PARTNERSHIPS

3. **Establish Clear Separation Between the Cyber Centre and CSE Obligations –** To protect the Cyber Centre's partnerships with operators, amendments to the bill should be made to prevent information shared with the Cyber Centre from being disclosed to other government departments and agencies, including the regulator.

LACK OF PROTECTION FOR REPORTING ENTITIES

4. **Introduce Clear Protections and 'Safe Harbour' for Disclosures –** Amend Bill C-8 to include provisions that prevent cybersecurity information shared with the government from being used for regulatory, enforcement, or legal actions. This will help preserve trust, encourage collaboration, and improve Canada's ability to respond to cyber threats.

CONCERN #1: REGULATORY DUPLICATION

Bill C-8 risks creating a duplicative regulatory framework for cybersecurity in the electricity sector, which is already governed by the North American Electric Reliability Corporation (NERC) and provincial regulators.

- Bill C-8 proposes to regulate assets and systems that are already subject to existing requirements under the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards. These standards have been widely adopted, enforced, and audited by most provincial regulators.
- NERC CIP standards already require operators to identify, categorize, and protect critical cyber assets and systems; conduct personnel risk assessments for individuals accessing critical systems; report certain cyber incidents; and manage supply chain risks. *(See Annex A for a list of NERC CIP standards.)*
- Some provincial frameworks also overlap with Bill C-8. For instance, the amended Ontario Cyber Security Standard now mandates that transmission and distribution entities report cybersecurity incidents.
- The risk of duplication and overlap across key aspects of Bill C-8 is significant. Before introducing new regulatory requirements for the electricity sector, the government should clearly explain how Bill C-8 will enhance cybersecurity beyond what is already provided by NERC CIP and provincial regulations.
- Duplicative regulatory requirements can lead to poor security outcomes. They increase compliance costs, create ambiguity and confusion, and divert resources away from actual security efforts. This is the potential impact of Bill C-8 on the electricity sector.

RECOMMENDATIONS

1. **Recognize Equivalent Regulatory Frameworks** – Include provisions that allow the regulator to acknowledge and accept compliance with equivalent frameworks. For example, electricity operators could fulfill Bill C-8's requirements for cybersecurity programs and supply chain risk management through their existing compliance with NERC CIP standards.
2. **Harmonize Incident Reporting Requirements** – Include provisions enabling the Governor in Council to establish mechanisms that align Bill C-8's incident reporting requirements with existing provincial and NERC CIP processes. Harmonization is essential to ensure timely and effective reporting, allowing operators to concentrate their efforts on incident response and recovery.

CONCERN #2: RISKS TO CYBER CENTRE PARTNERSHIPS

Bill C-8 could harm the Cyber Centre's partnerships with critical infrastructure operators. Involving the Communications Security Establishment (CSE) in advising regulators and informing cyber security directives risks discouraging operators from openly sharing information with the Cyber Centre, which spent years carefully building trusted relationships with critical infrastructure sectors. Allowing information shared in confidence with the Cyber Centre to be disclosed to a regulator will weaken collaboration, undermining trust that took years to build, and dissuading companies from sharing intelligence and seeking assistance.

- By requiring the CSE to share incident reports to the regulator, operators who may have sought the Cyber Centre's assistance in responding to an incident may now limit the volume and type of information they share during cyber incidents, shifting from open collaboration to cautious, legally vetted reporting, hindering collaboration during a crisis.

- Bill C-8 also requires the CSE to provide advice, guidance or services to the regulator as it seeks to ensure an operator's compliance with the mitigation of supply-chain or third-party risks. This may reduce operators' willingness to discuss openly with the Cyber Centre about our sector's supply chain risks, as it could potentially expose them to compliance actions.

- Bill C-8 authorizes CSE staff to share information with other government departments and agencies for the purpose of issuing cyber security direction. This has the potential to put a chill on all voluntary information shared with the Cyber Centre, as discussing vulnerabilities may cause the production of a direction.

- The relationship between NERC and the Electricity Information Sharing and Analysis Center (E-ISAC) is an example of how trust can be built with critical infrastructure operators while fulfilling regulatory requirements. While the E-ISAC is operated by NERC, it is organizationally isolated from its enforcement processes, ensuring that information reported to the E-ISAC is not be shared with NERC.

RECOMMENDATION

3. **Establish Clear Separation Between the Cyber Centre and CSE Obligations** – To protect the Cyber Centre's partnerships with operators, amendments to the bill should be made to prevent information shared with the Cyber Centre from being disclosed to other government departments and agencies, including the regulator.

CONCERN #3: LACK OF PROTECTION FOR REPORTING ENTITIES

Bill C-8 does not provide adequate protection from legal, regulatory or enforcement actions for entities that disclose cyber incidents or vulnerabilities to the government. This disincentivizes additional voluntary disclosures and represents a missed opportunity to implement *safe harbour* provisions and strengthen Canada's resilience to cyber threats.

- Legal and regulatory protections are a prerequisite to fostering trust between industry and government. When operators trust that their disclosures will not lead to enforcement actions, they are more likely to share meaningful information that strengthens Canada's cybersecurity posture.
- Without clear protections or *safe harbour* provisions, operators may limit their reporting and information sharing to only what is legally required, reducing the effectiveness of collaboration before and during cyber incidents. This chilling effect undermines the Cyber Centre's ability to support operators.
- Legislators should consider the kind of behaviour they want to encourage. If they want to encourage partnership and collaboration between industry and government, protections for mandated and voluntary disclosures are critical.
- Allowing information sharing between the regulator and the Cyber Centre, without clear *safe harbour* provisions, will not make critical infrastructure sectors more secure. It will impede communication, and disincentivize companies from seeking assistance and share information, for no regulatory enforcement benefit.

RECOMMENDATION

4. **Introduce Clear Protections and 'Safe Harbour' for Disclosures** – Amend Bill C-8 to include provisions that prevent cybersecurity information shared with the government from being used for regulatory, enforcement, or legal actions. This will help preserve trust, encourage collaboration, and improve Canada's resilience and ability to respond to cyber threats.

ANNEX A – NERC CIP STANDARDS

- CIP-002: BES Cyber System Categorization
- CIP-003: Security Management Controls
- CIP-004: Personnel & Training
- CIP-005: Electronic Security Perimeter(s)
- CIP-006: Physical Security of BES Cyber Systems
- CIP-007: System Security Management
- CIP-008: Incident Reporting and Response Planning
- CIP-009: Recovery Plans for BES Cyber Systems
- CIP-010: Configuration Change Management and Vulnerability Assessments
- CIP-011: Information Protection
- CIP-012: Communications between Control Centers
- CIP-013: Supply Chain Risk Management
- CIP-014: Physical Security