May 9, 2022

Vanessa Countryman, Secretary
Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-1090

Re: File Number S7-09-22, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

Dear Ms. Countryman:

Enbridge Inc. (Enbridge) appreciates the opportunity to provide comments to the Securities and Exchange Commission (the Commission) in response to the Commission’s request for public input on the Commission’s proposed rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure1 (the Proposed Rules).

Enbridge is a leading North American energy infrastructure company with common shares listed on the Toronto Stock Exchange and the New York Stock Exchange. We safely and reliably deliver the energy people need and want to fuel quality of life. Headquartered in Calgary, Alberta, Canada, our core businesses include Liquids Pipelines, which transports approximately 30 percent of the crude oil produced in North America; Gas Transmission and Midstream, which transports approximately 20 percent of the natural gas consumed in the U.S.; Gas Distribution and Storage, which serves approximately 3.9 million retail customers in Ontario and Quebec; and Renewable Power Generation, which owns approximately 1,766 MW (net) in renewable power generation capacity in North America and Europe.

We believe that cybersecurity attacks can have serious effects on critical infrastructure and national security, with the potential for systemic effects on the economy as a whole. This is a widely shared concern, and as the Commission will be aware, other government agencies have also taken action in response to this risk, including the Nuclear Regulatory Commission, the Federal Energy Regulatory Commission, the Transportation Security Agency (TSA) and the Cybersecurity and Infrastructure Security Agency (CISA).

At Enbridge, safety is a core value and a top priority. As an owner and operator of critical energy infrastructure, cybersecurity is an important risk consideration for Enbridge. Enbridge plays a critical role in enabling the economic well-being and quality of life of North Americans who depend on access to reliable energy. We are keenly aware that any interruptions in our business could impact energy supply to North Americans. We believe the detailed disclosures that would be required under the Proposed Rules could give malicious threat actors valuable insights into a company’s cybersecurity posture, with the unintended result of making the company more vulnerable to cyber-attacks. If the disclosure requirements are too extensive, they may exceed the Commission’s rulemaking authority and not survive legal challenges. We urge the Commission to carefully balance its investor protection policy goals against the harm of increased cybersecurity risks. It is in that spirit that Enbridge offers the following comments for consideration.

Material Cybersecurity Incident Disclosure and Updated Incident Disclosure

Materiality
Enbridge strongly believes that any Commission guidance or rulemaking regarding cybersecurity disclosure must support its statutory mission: to protect investors; maintain fair, orderly and efficient markets; and facilitate capital formation. Enbridge recognizes that material cybersecurity risks have become increasingly important to investors and other stakeholders. As the Commission has noted, public companies are already subject to disclosure requirements that include material cybersecurity risks and incidents. We believe that the concept of materiality is critical to maintain in any disclosure rules and guidance that the Commission chooses to implement. We believe further that companies are best positioned to determine which occurrences constitute material cybersecurity incidents for their business, and which details regarding these incidents or the company’s cybersecurity risk management, strategy and governance are material. We urge the Commission not to require disclosure of immaterial information that may not be decision-useful to investors, but that may pose a significant reporting burden on companies and expose them to greater risk of cyber-attack.

Definition of Cybersecurity Incident
We believe the Proposed Rules define “cybersecurity incident” too broadly, particularly when this term and the included term “information systems” are construed broadly. We believe companies are best positioned to determine what constitutes a cybersecurity incident for their business and that it is impractical and unduly burdensome to define “cybersecurity incident” to include occurrences that have had no adverse impact on a company’s business, financial condition or results or operations. Companies would be required to consider in their disclosure processes a substantial number of occurrences that they may consider to be neither cybersecurity incidents nor material. For example, an “unauthorized occurrence” could potentially include a breach of a technology, records or security policy by an employee or service provider, such as leaving a file cabinet unlocked in an office. The definition includes the mere “jeopardizing”, as opposed to actually having an impact on, information systems or information. The reference to “any information residing therein” potentially includes vast amounts of information.

Individually Immaterial Cybersecurity Incidents
The Proposed Rules would require periodic reporting when a series of previously undisclosed, individually immaterial cybersecurity incidents have become material in the aggregate, including the effect on the registrant’s operations and incident remediation status. We are concerned about the potential for disclosure of immaterial information under this proposed requirement and respectfully request that the Commission consider eliminating it. If the Commission maintains this proposed requirement, we urge the Commission to provide more guidance. In the context of the digitalization of business operations and rapidly increasing prevalence of cyber-attacks in the ordinary course of business, we believe it is difficult and operationally

---

2 U.S. Securities and Exchange Commission: SEC.gov | About the SEC.
4 See supra note 1 at p. 41: “Cybersecurity incident means an unauthorized occurrence on or through a registrant’s information systems that jeopardizes the confidentiality, integrity, or availability of a registrant’s information system or any information residing therein” and “Information systems” means information resources, owned or used by the registrant, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the registrant’s information to maintain or support the registrant’s operations.”
challenging to define what is “material in the aggregate” when considering the number and types of cyber-attacks and cyber-attackers over an indefinite period of time. We believe additional guidance could help ensure disclosure of material information in a manner that is decision-useful to investors and operationally feasible for companies.

Security Concerns
The U.S. federal government has identified critical infrastructure sectors whose operation is vital to national security, public health and safety\(^5\) and, in order to protect and coordinate responses to cyber-attacks, owners and operators of this critical infrastructure, including Enbridge, already work closely with the CISA, TSA and other agencies of the federal government and are subject to disclosure requirements to those agencies. As an owner and operator of critical energy infrastructure, we are concerned that the highly prescriptive requirements of the Proposed Rules would require public disclosure of detailed, sensitive information that is valuable to malicious threat actors and cyber-attackers, thereby increasing cybersecurity risks. The Proposed Rules include, for example, the requirement to disclose the effect on the registrant’s operations and the incident remediation status. Detailed disclosures regarding a material cybersecurity incident, particularly before it is contained or remediated, or of a company’s cybersecurity policies or procedures, could be exploited by an attacker to exacerbate an ongoing attack, exploit perceived vulnerabilities, or progress the targeting or sophistication of future attacks, thereby putting companies, investors and others at further risk. Detailed updates to previously disclosed cybersecurity incidents, in particular material effects or future impacts to a registrant’s operations, incident remediation status and any changes to the registrant’s policies and procedures as a result of a cybersecurity incident, similarly provide information that could be exploited by cyber-attackers. We believe that substantially less prescriptive requirements could help mitigate these risks. We encourage the Commission ensure its approach to cybersecurity information reporting is coordinated with other federal agencies, such as CISA and TSA, including in relation to security considerations and administrative and cost burdens to companies from multiple reporting requirements.

Law Enforcement Exemption
The Proposed Rules do not provide for any exemption from disclosure of material cybersecurity incidents where another law enforcement agency is involved. We believe a law enforcement exemption is necessary to avoid undermining national, corporate or personal security interests. We respectfully encourage the Commission to reconsider its approach to investor protection superseding other considerations.

Thank-you for the opportunity to provide comments. We welcome additional opportunities to further engage with the Commission on this topic.

Sincerely,

Enbridge Inc.

(Signed) “Robert R. Rooney”

Robert R. Rooney, Q.C.
Executive Vice President & Chief Legal Officer

\(^5\) See e.g., Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience; see also Statement by President Biden on our Nation’s Cybersecurity (March 21, 2022 – Statements and Releases).