

BCE Inc.
1 Carrefour Alexander-Graham-Bell
Building A, 7th Floor
Verdun, Québec H3E 3B3
Canada

Rogers Communications Inc.
333 Bloor Street East, 7th Floor
Toronto ON M4W 1G9
Canada

TELUS Corporation
510 Georgia Street West
Vancouver BC V6B 0M3
Canada

Via Email

Ms. Vanessa Countryman,
Secretary,
U.S. Securities and Exchange Commission,
100 F Street,
Washington, DC 20549-1090,
United States.

May 9, 2022

Re: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (File No. S7-09-22)

Dear Ms. Countryman:

We appreciate the opportunity to respond to the recently proposed rules of the U.S. Securities and Exchange Commission (the "SEC") on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (Release Nos. 33-11038; 34-94382; IC-34529; File No. S7-09-22) (the "Proposed Rules").

BCE Inc. ("BCE"), Rogers Communications Inc. ("RCI") and TELUS Corporation ("TELUS") are Canadian corporations and are the largest communications service providers in Canada. BCE, RCI and TELUS are also foreign private issuers ("FPIs") listed on the New York Stock Exchange and subject to U.S. periodic reporting requirements under the Securities Exchange Act of 1934, as amended (the "Exchange Act"). Further, BCE, RCI and TELUS are participants in the SEC's multijurisdictional disclosure system ("MJDS") for Canadian issuers, which allows eligible Canadian issuers, such as BCE, RCI and TELUS, to register securities under the U.S. Securities Act of 1933, as amended (the "Securities Act") and to register securities and satisfy their reporting obligations under the Exchange Act by use of documents prepared largely in accordance with Canadian requirements. As MJDS registrants, BCE, RCI and TELUS satisfy their reporting obligations under the Exchange Act by filing their respective annual reports on Form 40-F and other documents under cover of Form 6-K.

We note that the Proposed Rules did not contemplate any amendments to the current Form 40-F disclosure requirements. In its release, the SEC acknowledged that the MJDS generally permits eligible Canadian FPIs to use Canadian disclosure standards and

documents to satisfy the SEC's registration and disclosure requirements. However, the SEC specifically requested comment on whether MJDS registrants should be required to include the same cybersecurity disclosures in their annual reports on Form 40-F as would be required for U.S. domestic registrants for their annual reports on Form 10-K or other FPIs for their annual reports on Form 20-F.

Since the adoption by the SEC of the MJDS, MJDS registrants have been deemed to comply with the requirements of Regulation 13A pursuant to Rule 13a-3 (§ 240.13a-3 (*Reporting by Form 40-F Registrant*)). Rule 13a-3 has been effective since July 1, 1991 and was adopted in connection with the implementation of the MJDS framework. Rule 13a-3 specifies that "[a] registrant that is eligible to use Forms 40-F and 6-K and files reports in accordance therewith shall be deemed to satisfy the requirements of Regulation 13A (§§ 240.13a-1 through 240.13a-17 of this chapter)." The SEC's regulations would otherwise require MJDS registrants to comply with the SEC's prescriptive disclosure requirements in accordance with the applicable SEC's form requirements (*e.g.*, annual reports on Form 20-F for FPIs). The SEC noted in its decision to adopt MJDS that:

> *Canada was chosen as the first partner for the United States in part because of the similarities between the U.S. and Canadian investor protection mandates and disclosure requirements. The existence of a well-developed, sophisticated and reliable system of administering Canadian disclosure requirements also was critical, given the Commission's reliance on Canadian definitions, procedures, application of disclosure standards, and day-to-day administration of those standards.*[1]

The MJDS framework appropriately treats the Canadian reporting framework as substantially equivalent to that of the SEC, avoids duplicative and overlapping reporting obligations, and acknowledges that Canadian reporting requirements are sufficient for investors in the United States. We note that MJDS forms will continue to specify that an MJDS registrant must include information in its filings such that its disclosures do not contain material misstatements or omissions.[2] We therefore believe the existing disclosure framework for MJDS registrants is sufficient to inform U.S. investors of material cybersecurity incidents.

Accordingly, we strongly support the SEC's approach of not amending Form 40-F in the Proposed Rules,[3] since imposing prescriptive reporting requirements on MJDS registrants

---

1 SEC Release No. 33-6879, 55 Fed. Reg. 46,288, 46,288–89 (Nov. 2, 1990).

2 See, e.g., General Instruction D(5) to Form 40-F (specifying that Rule 12b-20 under the Exchange Act applies for reports filed on such form).

3 Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 87 Fed. Reg. 16590 (Mar. 23, 2022) (to be codified at 17 C.F.R. pt. 229, 232, 239, 240, and 249), at 16603 ("We are not

with respect to cybersecurity topics would be completely inconsistent with the fundamental principles of the MJDS. Extending these new cybersecurity disclosure requirements to MJDS registrants would result in an unnecessary and inefficient incremental burden for registrants already subject to a robust reporting regime in Canada, exactly the situation that MJDS was designed to avoid. Consistent with the SEC's existing approach to disclosure requirements, we support excluding MJDS registrants from the new annual reporting requirements under the Proposed Rules. MJDS registrants would continue to file annual reports on Form 40-F consistent with past practice and furnish information on Form 6-K to the extent required under the existing MJDS disclosure framework.

We note that Canadian securities regulators have been focused on cybersecurity disclosures for a number of years. For example, the Canadian Securities Administrators (the "CSA") identified cybersecurity as a priority area in the CSA's 2016-19 Business Plan. The CSA has since issued extensive guidance on disclosure of material cybersecurity incidents and cybersecurity risk management practices of Canadian reporting companies and published numerous notices highlighting the importance of cybersecurity to Canadian financial markets and the need for prevention, coordination and remediation plans.[4] We understand that cybersecurity matters continue to be an active priority for the CSA[5] and that the members of the CSA consider cybersecurity matters as part of their ongoing continuous disclosure reviews applicable to Canadian issuers. We therefore believe the existing disclosure framework for MJDS registrants is sufficient to inform U.S. investors of material cybersecurity incidents.

Finally, we wanted to express a specific concern with the current scope of the Proposed Rules. We understand that, for U.S. domestic registrants, the Proposed Rules would impose prescriptive requirements for the timing and content of disclosure of material cybersecurity incidents, and additional disclosure requirements, without regard for the security risks and harms that such disclosures may pose in certain circumstances. We (like many other companies) rely on a variety of third party IT products and services which may be provided by U.S. domestic registrants. In our view, no registrant should be required to disclose an ongoing or unremediated incident, and periodic disclosures should

---

proposing any changes to Form 40-F. Should we instead require an MJDS issuer filing an annual report on Form 40-F to comply with the Commission's specific proposed cybersecurity-related disclosure requirements in the same manner as Form 10-K or Form 20-F filers?").

4 See, e.g., CSA Staff Notice 11-326, *Cyber Security* (September 26, 2013); CSA Staff Notice 11-332, *Cyber Security* (September 27, 2016); CSA Multilateral Staff Notice 51-347, *Disclosure of cyber security risks and incidents* (January 19, 2017); CSA Staff Notice 11-336, *Summary of CSA Roundtable on Response to Cyber Security Incidents* (April 6, 2017); CSA Staff Notice 11-338, *CSA Market Disruption Coordination Plan* (October 18, 2018).

5 See, e.g., CSA Interim Progress Report 2021 and OSC Business Plan for the fiscal years ending 2023-2025.

not require registrants to disclose progress in remediation or the nature of remediation activities, where such disclosures may harm the registrant or its customers, or conflict with the requests of law enforcement officials. Requiring registrants to disclose ongoing and unremediated incidents or the nature and progress of remediation activities may allow the original malicious actors to engage in techniques to hide their presence in the work, making it difficult to detect them, and allow the original malicious actors or others to exploit the IT product or service provider further and attack its customers. This increases the likelihood that we or other similarly situated customers could experience material cybersecurity incidents as a direct result of the disclosure of an ongoing and unremediated incident or disclosure of the nature and progress of remediation activities. This result is not in the interests of the affected registrants, their shareholders or their customers (such as BCE, RCI and TELUS).

* * *

We thank you for the opportunity to provide our views on the Proposed Rules. In response to the SEC's request for comment, we confirm that no prescriptive cybersecurity disclosure requirements should be required for MJDS registrants filing their annual reports on Form 40-F.

Very truly yours,

BCE Inc.

Robert Malcolmson
Executive Vice-President,
Chief Legal and Regulatory Officer

Rogers Communications Inc.

Ted Woodhead
Chief Regulatory Officer and Government Affairs

TELUS Corporation

Andrea Wood
Chief Legal and Governance Officer