CAMECO CORPORATION
Corporate Office
2121 – 11th Street West
Saskatoon, Saskatchewan
Canada S7M 1J3

Tel 306.956.6200
Fax 306.956.6201
www.cameco.com

November 1, 2022

VIA EMAIL

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

Dear Ms. Countryman:

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

Thank you for the opportunity to review and comment on the Securities and Exchange Commission's (SEC) proposed rule: **Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure** (File Number S7-09-22).

Cameco supports the SEC's desire to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance and cybersecurity incident reporting by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934, as amended ("The Exchange Act").

Cameco is a Canadian corporation and is also a foreign private issuer listed on the New York Stock Exchange, and it is therefore subject to U.S. periodic reporting requirements under the Exchange Act. Further, Cameco is a participant in the SEC's multijurisdictional disclosure system ("MJDS") for Canadian issuers, which allows eligible Canadian issuers, such as Cameco to register securities under the U.S. Securities Act of 1933, as amended (the "Securities Act") and to satisfy its reporting obligations under the Exchange Act by use of documents prepared largely in accordance with Canadian requirements. As MJDS registrants, Cameco satisfies its reporting obligations under the Exchange Act by filing its 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.

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.[1] We therefore believe the existing disclosure framework for MJDS registrants is sufficient to inform U.S. investors of material cybersecurity risks, strategy, governance, and incidents.

Accordingly, we strongly support the SEC's approach of not amending Form 40-F in the proposed rules. We believe imposing prescriptive reporting requirements on MJDS registrants with respect to cybersecurity topics would result in an unnecessary and inefficient incremental burden for registrants already subject to a robust reporting regime in Canada, which is inconsistent with the fundamental principles of the MJDS.

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.[2] We understand that cybersecurity matters continue to be an active priority for the CSA[3] 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 risks, strategy, governance, and incidents.

As a result, we strongly suggest that SEC maintains its initial position and not propose any changes to Form 40-F. This position best supports the proposed intent of both the SEC and CSA proposals in their efforts to enable information standardization and comparability for informed investor decision making while balancing increasing reporting and disclosure labour and cost burdens for reporting issuers.

If you would like to discuss this further, then please contact me at [redacted] or by email at [redacted].

Sincerely,

Alice Wong
Senior Vice-President and Chief Corporate Officer
CAMECO CORPORATION

c: Rachelle Girard
Vice-President, Investor Relations, Treasury & Tax

---

[1] 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).
[2] 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).
[3] See, e.g., CSA Interim Progress Report 2021 and OSC Business Plan for the fiscal years ending 2023-2025.