Council of Institutional Investors®
The voice of corporate governance

Via E-Mail

May 9, 2022

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

Re: *File No. S7-09-22*

Dear Madam Secretary:

I am writing of behalf of the Council of Institutional Investors (CII) in response to the Securities and Exchange Commission's (SEC or Commission) proposed new rules (the Proposal or Proposed Rules) on cybersecurity risk management, strategy, governance and incident disclosure.[1]

CII is a nonprofit, nonpartisan association of United States (U.S.) public, corporate and union employee benefit funds, other employee benefit plans, state and local entities charged with investing public assets, and foundations and endowments with combined assets under management of approximately $4 trillion. Our member funds include major long-term shareowners with a duty to protect the retirement savings of millions of workers and their families, including public pension funds with more than 15 million participants – true "Main Street" investors through their pension funds. Our associate members include non-U.S. asset owners with about $4 trillion in assets, and a range of asset managers with more than $40 trillion in assets under management.[2]

As the leading voice for effective corporate governance and strong shareholder rights, CII generally supports the content and goals of the Proposed Rules, as they would enhance the detail and usefulness of cybersecurity disclosure to investors, while making filings more timely, consistent and locatable.

We believe the Proposal builds upon and enhances the Commission's February 2018 Statement and Interpretative Guidance on Public Company Cybersecurity Disclosures (2018 Interpretive

[1] See Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure: 87 Fed. Reg. at 16,590-16,624 (proposed Mar. 23, 2022), https://www.federalregister.gov/documents/2022/03/23/2022-05480/cybersecurity-risk-management-strategy-governance-and-incident-disclosure.

[2] For more information about the Council of Institutional Investors ("CII"), including its board and members, please visit CII's website at http://www.cii.org.

Release) by improving the ability of investors to analyze risk at the company level, while also conveying systemic benefits to investors, consumers and U.S. economic security.[3]

Systemic cybersecurity risks are a significant concern to the U.S. markets and economy.[4] Operating in today's world involves data security challenges that must be managed with appropriate and substantial security investments by public companies for the health and safety of the markets. We believe the disclosed information will not only better inform investors but also provide incentives for companies to implement effective cybersecurity strategies.

Disclosure regarding the board of directors' cybersecurity expertise

CII has previously commented on matters of cybersecurity, specifically on governance structures to mitigate cybersecurity risk.[5] We believe that cybersecurity is an integral component of a board's role in risk oversight[6], and recently our members voted to incorporate this and to reference material cybersecurity risks in our member-approved Corporate Governance Policies.[7]

The Proposal acknowledges that the expertise of the board in overseeing risk management, strategy and governance decisions around cybersecurity is important information for investors. Directors have the authority, capacity and responsibility to make pivotal contributions in this area by ensuring adequate resources and management expertise are allocated to robust cyber risk management policies and practices, and ensuring disclosure fairly and accurately portrays material cyber risks and incidents.[8] To achieve these objectives, directors need to:

- Understand management's cybersecurity strategy;
- Learn where cybersecurity weaknesses lie and;

[3] Press Release 2018-22, SEC Adopts Statement and Interpretative Guidance on Public Company Cybersecurity Disclosures (Feb. 21, 2018), https://www.sec.gov/news/press-release/2018-22.
[4] Cyber-Risk Oversight 2020 Key Principles and Practical Guidance for Corporate Boards, by the Internet Security Alliance and NACD, http://isalliance.org/wp-content/uploads/2020/02/RD-3-2020_NACD_Cyber_Handbook__WEB_022020.pdf. See also Cost of a Data Breach Report 2021, by IBM, https://www.ibm.com/downloads/cas/OJDVQGRY and What Companies are disclosing about cybersecurity risk and oversight, August 2020, by EY Center for Board Matters, https://www.ey.com/en_us/board-matters/what-companies-are-disclosing-about-cybersecurity-risk-and-oversight.
[5] Letter from Ken Bertsch, Executive Director, Council of Institutional Investors to The Honorable Jack Reed, United States Senate (July 7, 2017), https://www.cii.org/files/07_07_17%20letter%20to%20Senator%20Reed.pdf. See also Letter from Jeff Mahoney, General Counsel, Council of Institutional Investors, to The Honorable Michael Crapo, Chairman, Committee on Banking, Housing, and Urban Affairs et al. 6-7 (June 27, 2018) (sharing CII views on cybersecurity and related legislation), https://www.cii.org/files/June%2027%202018%20Letter%20to%20Senate%20Banking%20(final).pdf. See also letter from Jeff Mahoney, General Counsel, Council of Institutional Investors to Nicole Puccio (July 19, 2018) (sharing views on Draft 2018-2022 Strategic Plan), https://www.cii.org/files/July%2019%202018%20SEC%20Strategic%20Plan%20final%20(003).pdf.
[6] CII, Prioritizing Cybersecurity, Five Investor Questions for Portfolio Company Boards 2 (Apr. 2016), https://www.cii.org/files/publications/misc/4-27-16%20Prioritizing%20Cybersecurity.pdf.
[7] CII, Corporate Governance Policies, last updated March 2022; updated to reflect cybersecurity risk in September 2021, see Sections 2.12a Informed Directors and 2.7 Board's Role in Strategy and Risk Oversight, https://www.cii.org/files/03_07_22_corp_gov_policies.pdf.
[8] CII, Prioritizing Cybersecurity, 2016.

- Support informed, reasonable investment in the protection of critical data and assets.[9]

To cast informed votes on directors, CII members and other institutional investors need the information described in the Proposal to ensure that their representatives are accomplishing these objectives. Specifically:

- We are pleased to see that the Proposed Rules address the role of the board in cybersecurity risk management and strategy in a thorough manner, including disclosure of whether any board member has expertise or experience in cybersecurity.

- We support the adoption of proposed Item 407(j)(2) safe harbor, which ensures board members with cybersecurity expertise will not be subject to a higher level of liability than other directors.

- We believe disclosing the names of board members with cyber expertise is unlikely to deter such members from performing board service. These skills are highly sought after, and coupled with the proposed Item 407(j)(2) safe harbor and the understanding that cybersecurity is the responsibility of the full board, board members with this expertise should not expect higher risk from their service and therefore not be deterred.

- We believe that annual disclosure of cyber expertise among board members, if any, in the annual report and proxy would be helpful to investors, especially in voting decisions.

Disclosure of cybersecurity incidents in Form 8-Ks and periodic reports

The Proposal codifies directives in the 2018 Interpretive Release on the timing of filings and the scope of information companies need to relay to investors, markets, peers, customers and regulators when attacks or threats have risen to a material level. In the absence of the more specific requirements in the Proposal, many companies likely will continue to provide inadequate information on their processes, responses and level of vulnerability, as noted in the Proposal.[10] The lack of timely, comprehensive disclosure of material cyber events exposes investors and the community at large to potential harm. Specifically:

- We agree that investors would benefit from current reporting about material cybersecurity incidents on Form 8-K.

[9] *Id.*
[10] 87 Fed. Reg. at 16,603, "…the staff has observed certain cybersecurity incidents that were reported in the media but that were not disclosed in a registrant's filings."

- We believe the balance between informational needs of investors and the reporting burdens on registrants is appropriate.

- We believe the exclusion of specific technical information relevant to vulnerabilities and planned responses is appropriate. We are comfortable with the date of initial materiality determination as the defining disclosure trigger.

- We do not oppose a delay in filing based on the Attorney General's written determination that the delay is in the interest of national security.

- We support disclosure of substantial updates with material changes in continued reporting of prior incidences in Form 8-K. Other updates of non-material significance could be accomplished with regularly scheduled filings.

- We agree with the requirement to disclose smaller and/or frequent attacks that become "material in the aggregate."

The Proposal has goals of protecting investors and incenting a more robust framework of cybersecurity defense within our capital markets. As Chair Gensler recently said, "Cyber relates to each part of our three-part mission: investor protection, facilitating capital formation, and that which is in the middle, promoting fair, orderly, and efficient markets."[11] CII agrees.

Thank you for considering CII's views. If we can answer questions or provide additional information, please do not hesitate to contact me at tracy@cii.org.

Sincerely,

Tracy Stewart
Director of Research

[11] Remarks by Gary Gensler Before the Joint Meeting of the Financial and Banking Information Infrastructure Committee and the Financial Services Sector Coordinating Council, https://www.sec.gov/news/speech/gensler-speech-joint-meeting-041422.