United States Senate
WASHINGTON, DC 20510

May 9, 2022

Via Electronic Mail

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

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

Dear Ms. Countryman:

We write to respectfully request that the Securities and Exchange Commission (SEC) finalize, as proposed, rules requiring periodic disclosures by public companies regarding cybersecurity expertise on their boards of directors and management's role in implementing cybersecurity policies and procedures (the Proposal).

The Proposal would implement bipartisan legislation that we have introduced called the Cybersecurity Disclosure Act. That legislation directs the SEC to issue rules requiring each public company to disclose, in its annual report or annual proxy statement, whether any member of its governing body has expertise or experience in cybersecurity, including details necessary to describe fully the nature of that expertise or experience. And if no member has such expertise or experience, a company would be required to describe what other aspects of the company's cybersecurity were considered by any person, such as an official serving on a nominating committee, who is responsible for identifying and evaluating nominees for membership to the governing body.

The Proposal follows the intent of our bill by encouraging directors to play a more effective role in cybersecurity risk oversight at public companies, and we commend the SEC for issuing a Proposal that would achieve this important goal.

We respectfully request that the SEC finalize Items 106(c) and 407(j) of Regulation S-K as proposed. Item 106(c) would require disclosure about public companies' cybersecurity governance, including the board's oversight of cybersecurity risk and a description of management's role in assessing and managing cybersecurity risks, the relevant experience of management, and its role in implementing cybersecurity policies, procedures, and strategies. Item 407(j) would require disclosure about the cybersecurity expertise of members of the board of directors, if any, including the name of any director, and details to describe the nature of the expertise.

I. Cybersecurity is an important component of long-term shareholder value.

Cybersecurity incidents have never been more frequent, complex, and costly. Last year, the overall number of data breaches reached an all-time high of 1,862, up 23% year-over-year.[1] Almost all of these data breaches were caused by cyberattacks. The average cost of a data breach has also reached an all-time high last year of $4.24 million, up 10% year-over-year.[2] To take one concrete example at the high end of this scale, the Equifax breach in 2017 ultimately cost the company over $1.7 billion.[3] Companies of all sizes and in many industries have experienced serious cybersecurity incidents with significant impacts on customers, counterparties, and investors.

Investors often bear the costs associated with these incidents. The Proposal details a number of specific costs to companies and shareholders, including payments to meet ransom, liability for stolen information, increased insurance premiums, lost revenues due to theft of intellectual property, reputational damage, and litigation costs.[4] These costs culminate in damage not only to a company's profitability, but also to its stock price. According to a report by leading economic consulting firms, a severe cybersecurity breach causes an average permanent decline in a company's valuation of 1.8%.[5] The Proposal would provide investors with the disclosure they deserve regarding how public companies plan to guard against these risks before they materialize.

II. The Proposal provides powerful incentives for public companies to bolster cybersecurity, preserving long-term shareholder value.

Prudent management of cybersecurity risk is important to maintaining long-term shareholder value. Directors therefore have a responsibility to manage this risk and contribute to a company's cybersecurity. But corporate boards are struggling to meet this important obligation. Only 40% of boards have a director with cybersecurity experience.[6] And a recent survey by consulting firm EY confirmed a "deficiency of cybersecurity expertise at the C-suite level."[7] Indeed, according to a recent survey, 60% of directors "don't believe that cybersecurity should get in the way of business operations."[8] The Proposal appropriately recognizes that boards must be more vigilant because cybersecurity is among the most significant challenges companies face.

---

[1] Identity Theft Resource Center, *Annual Data Breach Report* (2022), at 5.
[2] IBM Security, *Cost of a Data Breach Report* (2021), at 4, https://www.ibm.com/downloads/cas/OJDVQGRY.
[3] Ben Lane, Housingwire, *Equifax Expects to Pay Out Another $100 Million for Data Breach*, February 14, 2020, https://www.housingwire.com/articles/equifax-expects-to-pay-out-another-100-million-for-data-breach/.
[4] Proposal, at 16592.
[5] CGI, *The Cyber-Value Connection; Revealing the Link Between Cyber Vulnerability and Company Value* (Aug. 2018), at 6, https://www.cgi.com/sites/default/files/2018-08/cybervalueconnection_full_report_final_lr.pdf.
[6] National Association of Corporate Directors and the Internet Security Alliance, *Cyber-risk Oversight: Key Principles and Practical Guidance for Corporate Boards* (2020), at 68, http://isalliance.org/wp-content/uploads/2020/02/RD-3-2020_NACD_Cyber_Handbook__WEB_022020.pdf.
[7] Chuck Seets, EY, *Cybersecurity: Staying Vigilant Through Prevention, Oversight and Governance*, January 18, 2022, https://www.ey.com/en_us/assurance/cybersecurity-staying-vigilant-through-prevention-oversight-and-governance.
[8] National Association of Corporate Directors, Public Company Governance Survey (2020), at 19, https://corpgov.law.harvard.edu/wp-content/uploads/2020/01/2019-2020-Public-Company-Survey.pdf.

The Proposal would create powerful incentives for public companies to pay greater attention to cybersecurity risks. According to a report by the prior Administration's Council of Economic Advisors, "mandatory disclosure requirements were previously shown to incentivize firms to adopt better cybersecurity measures."[9] The Proposal's board-level expertise disclosure requirement is a prime example of such an incentive. The North American Securities Administrators Association agrees that "[i]ncentivizing publicly traded companies to consider whether or not they have appropriate cybersecurity expertise on their governing body is a common-sense way to promote greater attention to cybersecurity risk by public corporations. Investors and customers are well-served by policies that encourage companies to consider such risks proactively, as opposed to after a data breach has already occurred, when such investors and customers have already been harmed."[10] Proposed Item 106(c) of Regulation S-K would direct public companies to provide these exact disclosures.

The disclosures in the Proposal will also enable investors to hold public companies accountable. In a letter of support for the Cybersecurity Disclosure Act, the Council of Institutional Investors stated its belief that "cybersecurity is an integral component of a board's role in risk oversight."[11] In another letter of support, the California Public Employees' Retirement System said that this approach will "ensure that investors have access to decision-useful information to better assess the ability of corporate management to adequately address cybersecurity risks."[12] And according to consulting firm EY, "remaining cyber-resilient and building stakeholder trust in the company's data security and privacy practices is a strategic imperative. Public disclosures can help build trust by providing transparency and assurance around how boards are fulfilling their cybersecurity risk oversight responsibilities."[13] If public companies provide the market with more insights into their governance of cybersecurity risks, then investors will be better equipped to decide whether to invest in a public company and how to vote in elections for directors.

III. Cybersecurity poses unique risks to public companies, which justify the disclosures required by the Proposal.

The unique harms caused by cybersecurity breaches justify the Proposal. According to testimony by Professor John Coates of Harvard Law School before the Senate Banking Committee:

> [T]here is maybe going to be some suggestion that there is a slippery slope and there is all kinds of risks and that cyber is one of them and so on. I really do want to emphasize that cyber is unique. Other than financial risk, where we already have an obligation for boards to say do they have financial expertise on the board or not,

[9] White House Council of Economic Advisers, *The Cost of Malicious Cyber Activity to the U.S. Economy* (Feb. 2018), at 25, https://nsarchive.gwu.edu/document/17664-council-economic-advisors-cost.
[10] Letter from North American Securities Administrators Association to Sen. Jack Reed, January 31, 2018.
[11] Letter from Council of Institutional Investors to Sen. Michael Crapo and Sen. Sherrod Brown, June 27, 2018.
[12] Letter from California Public Employees' Retirement System to Sen. Jack Reed, July 26, 2017.
[13] EY, *What Companies are Disclosing About Cybersecurity Risk and Oversight*, August 10, 2020, https://www.ey.com/en_us/board-matters/what-companies-are-disclosing-about-cybersecurity-risk-and-oversight.

> other than financial risk, cyber risk is, I believe, the one type of risk that is almost universal among public companies. It is very hard to think of a public company in this network age that is not at least somewhat exposed to cyber risk.[14]

This is precisely why cybersecurity risk warrants special attention from the SEC. The Proposal is narrowly tailored to require disclosure of board-level expertise that is important to mitigating this singular risk to public companies' profitability and valuation.

Moreover, the Proposal accomplishes this goal while providing appropriate discretion to public companies to define what constitutes "cybersecurity expertise" and to address cybersecurity risks through any means they see fit. The Proposal, like our legislation, does not mandate that any company's board actually have a person with expertise in cybersecurity or require companies to take any actions other than to provide this disclosure. We respectfully request that the SEC adopt this flexible disclosure approach over mandating any set of best practices, in order to encourage boards to develop approaches that are tailored to mitigate risks to the specific set of shareholders to which they are accountable.

* * *

Thank you for proposing rules to implement our bipartisan legislation. Please keep our staffs informed of the SEC's progress on improving cybersecurity disclosures by public companies.

Sincerely,

Jack Reed
United States Senator

Catherine Cortez Masto
United States Senator

Kevin Cramer
United States Senator

Angus S. King, Jr.
United States Senator

[14] Legislative Proposals to Examine Corporate Governance, Hearing Before the S. Comm. on Banking, Housing, and Urban Affairs, 115 Cong. 406 (statement of John C. Coates IV).

Ron Wyden
United States Senator

Mark R. Warner
United States Senator

Susan M. Collins
United States Senator