California Public Employees' Retirement System
Executive Office
400 Q Street, Sacramento, CA 95811 | Phone: [redacted] | Fax: [redacted]
888 CalPERS [redacted] | TTY [redacted] | **www.calpers.ca.gov**

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

May 9, 2022

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

Dear Secretary Countryman,

On behalf of the California Public Employees' Retirement System (CalPERS), I write to express our support for the Securities and Exchange Commission's (SEC or Commission) proposed rule to require public companies to periodically disclose information on their cybersecurity risk management, strategy, and governance practices, and report material cybersecurity incidents in a timely manner (Proposed Rule).

As the largest public defined benefit pension fund in the United States, we manage approximately $470 billion in global assets on behalf of more than 2 million members. As a global, institutional investor with a long-term investment horizon, we seek long-term sustainable, risk-adjusted returns through efficient capital allocation and stewardship in line with our fiduciary duty. Furthermore, we believe that all investors, whether large institutions or private individuals, should have access to disclosures that allow them to make informed proxy voting and investment decisions.

CalPERS' Investment Beliefs[1] recognize that long-term value creation requires effective management of three forms of capital: financial, physical, and human.[2] Accordingly, our fiduciary duty requires that we proactively assess whether the companies that we hold in our portfolio are managing capital effectively. Our Governance and Sustainability Principles[3] identify robust governance practices as being critical to long-term performance; therefore, we expect fair, accurate, timely, and assured reporting about how companies manage these three

[1] CalPERS Investment Beliefs, https://www.calpers.ca.gov/page/about/organization/calpers-story/our-mission-vision#investment-beliefs.
[2] Id.
[3] CalPERS Sustainability Principles, https://www.calpers.ca.gov/docs/forms-publications/governance-and-sustainability-principles.pdf.

forms of capital to generate sustainable returns, including how they identify, monitor, and mitigate risks. Moreover, these Principles hold that an effective risk oversight process considers both internal company-related risks such as operational, financial, credit, solvency, liquidity, corporate governance, **cybersecurity**, environmental, reputational, social, product safety; and external risks, such as geopolitical, industry related, systemic, and macro-economic. Given the widespread reliance of modern society on technology, cybersecurity is a risk that may have a material impact, to a greater or lesser extent, upon any of these aforementioned risks public companies must navigate.

We applaud the prior work of the SEC to highlight and clarify the disclosure obligations of public companies regarding their cybersecurity risks and incidents, including issuing interpretive guidance in 2011 and 2018. We also appreciate the Commission's recognition of the importance that investors place on cybersecurity, as evidenced by its proposed rulemaking for cybersecurity of investment advisors and investment companies[4] released earlier this year. We believe the boards of all companies, investment vehicles and external investment managers we invest in and do business with must be accountable for overseeing the use of our capital. It is their duty to ensure their companies function as "risk intelligent" organizations, and we believe the adoption and implementation of that proposed rulemaking will strengthen cybersecurity preparedness and improve the resilience of investment advisers and investment companies against cybersecurity threats and attacks.

I. RISK MANAGEMENT, STRATEGY & GOVERNANCE DISCLOSURE

Beginning with the Cybersecurity Disclosure Act of 2017 (S. 536 by Senator Jack Reed (D-RI))[5], we have consistently supported[6] legislative efforts to require publicly traded companies to disclose in their annual reports or annual proxy statements, whether any member of their governing body, such as a board of directors, has expertise or experience in cybersecurity issues. Similarly, the Proposed Rule would address the increasing prominence of cybersecurity threats in our financial markets and the broader economy by requiring the disclosure of cybersecurity expertise on corporate boards.

Specifically, we believe boards of directors "should set out specific risk tolerances and implement a dynamic process that continuously evaluates and prioritizes risks"[7] as detailed previously. Further, we agree with the Council of Institutional Investors (CII) that, "Effective cybersecurity risk management starts with the board. Users should expect companies of various sizes, industries and cyber risk profiles to bring different strategies, in varied stages of

[4] SEC Proposed Rule S7-04-22 – Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies. https://www.govinfo.gov/content/pkg/FR-2022-03-09/pdf/2022-03145.pdf.
[5] S. 536, 115th Congress. https://www.congress.gov/115/bills/s536/BILLS-115s536is.pdf.
[6] CalPERS Letter in Support of S. 536, dated July 26, 2017. https://www.calpers.ca.gov/docs/legislative-regulatory-letters/congress-senate-536-cybersecurity-disclosure-act-07-26-2017.pdf.
CalPERS Letter in Support of S. 808, dated April 2, 2021. https://www.calpers.ca.gov/docs/legislative-regulatory-letters/support-cybersecurity-disclosure-act-04-02-21.pdf.
[7] CalPERS Sustainability Principles, p.20. https://www.calpers.ca.gov/docs/forms-publications/governance-and-sustainability-principles.pdf.

implementation, in response to this massive and growing challenge."[8] We have advocated for board policies and voted our proxies in alignment with these CII recommendations on how boards of directors can effectively and efficiently ensure their companies have developed and implemented an effective cybersecurity risk management, strategy, and governance framework.[9] With this Proposed Rule, the Commission has taken a vital next step to ensure investors have access to periodic disclosures about a registrant's policies and procedures to identify and manage cybersecurity risk and the impact of these risks on business strategy; management's role and expertise in implementing cybersecurity policies, procedures, and strategies; and the board of directors' oversight role, and cybersecurity expertise, if any. Moreover, the proposed reporting regime for material cybersecurity incidents will allow investors to assess the effectiveness of public companies' cybersecurity-related policies and procedures.

Beyond supporting cybersecurity strategies that address internal company-related risks, ensuring board members' understanding of the cybersecurity landscape is also vital to their understanding of external company-related risks. We believe the board is ultimately responsible for a company's risk management philosophy, organizational risk framework and oversight. The board should be comprised of skilled directors with a balance of broad business experience and extensive industry expertise to understand and question the breadth of risks faced by the company.[10] Risks posed by cybersecurity incidents and threats should be understood by board members, and we have long advocated that board members should develop and have cybersecurity expertise.

II. INCIDENT REPORTING AND MATERIALITY

CalPERS enthusiastically supports the Commission's efforts to require current and periodic reporting of material cybersecurity incidents. We agree with the Commission's prior guidance that "if cybersecurity incidents or risks materially affect a company's products, services, relationships with customers or suppliers, or competitive conditions, the company must provide appropriate disclosure."[11] Cybersecurity incidents can have various material impacts on investment and proxy voting decisions; for example, a reasonable shareowner would likely consider information on cyberattack-induced product and service disruptions when making such decisions. Just last month, the U.S. Department of Energy and various U.S. intelligence agencies warned energy companies of new malware that targets electricity and natural gas infrastructure systems.[12] As part of an effective risk oversight process, cybersecurity considers both internal company-related risks and external risks, and any malware attack on a public company that provides energy to the American public should be disclosed to shareowners.

The Proposed Rule also includes requirements that registrants report certain cybersecurity incidents. We noted an example of a cyberattack causing a product or service disruption above,

---

[8] Council of Institutional Investors, *Prioritizing Cybersecurity*, April 2016 https://www.cii.org/files/publications/misc/4-27-16%20Prioritizing%20Cybersecurity.pdf.
[9] Id.
[10] CalPERS Total Fund Investment Policy, p.76. https://www.calpers.ca.gov/docs/total-fund-investment-policy.pdf.
[11] Commission Statement and Guidance on Public Company Cybersecurity Disclosures, February 26, 2018 https://www.sec.gov/rules/interp/2018/33-10459.pdf.
[12] U.S. warns energy firms of a rapidly advancing hacking threat, April 14, 2022 https://www.eenews.net/articles/u-s-warns-energy-firms-of-a-rapidly-advancing-hacking-threat/.

but many other types of cybersecurity incidents ought to be reported as material. For example, cyberattacks could ransom a registrant's customers' confidential information in exchange for cryptocurrency. These kinds of incidents can be time-sensitive and can lead to direct harm to a registrant's customers, impacting the registrant's reputation and bottom line in the process.

The Commission's past guidance, while in line with our views, does not go far enough. The Proposed Rule is needed to provide clarity regarding what, when, and how to disclose material cybersecurity incident information. Commission staff appropriately noted that current reporting is "inconsistent, may not be timely, and can be difficult to locate."[13] The improved standardization of disclosures included in the Proposed Rule adds clarity to the reporting process.

III. CONCLUSION

CalPERS supports the adoption and implementation of the Proposed Rule to require periodic disclosures of registrants' risk management, strategy, and governance regarding cybersecurity risks, as well as more complete and timely disclosures of material cybersecurity incidents, because it ensures that investors have access to crucial decision-making information to better assess the ability of corporate management to adequately address cybersecurity risks. Moreover, it helps to promote capital market efficiency by providing greater insight into the extent to which companies are focused on data security and the protection of consumer information.

Thank you for the opportunity to share our comments. If you have any questions or wish to discuss in more detail, please do not hesitate to contact James Andrus, Interim Managing Investment Director, at [redacted] or [redacted].

Sincerely,

Marcie Frost
Chief Executive Officer

cc: James Andrus

[13] Proposed Rule, https://www.sec.gov/rules/proposed/2022/33-11038.pdf