Empowering Directors. Transforming Boards.

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

Re: File Number S7-09-22

May 9, 2022

Dear Ms. Countryman:

The National Association of Corporate Directors (NACD) is pleased to comment on the recent rulemaking release describing proposed rules on "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure."[i] As the nation's leading organization for director education and certification, with a membership of more than 23,000, NACD extends its support for many of the proposed concepts in this Release. We also encourage the SEC to revise a few concepts.

We have made our support for board-level oversight of cybersecurity and attendant risks clear in NACD's handbook on *Cyber-Risk Oversight* (February 2020),[ii] produced in collaboration with the Internet Security Alliance (ISA). Citing the NACD-ISA handbook, the Release notes that "senior management and boards of directors of public companies have become increasingly concerned about cybersecurity threats." (Release, Note 14), and further that to "mitigate the potential costs and damage that can result from a material cybersecurity incident, management and boards of directors may establish and maintain effective risk management strategies to address cybersecurity risks" (Proposed Rule, Note 20). Furthermore, the Release appropriately cites NACD's report on *The State of Cyber-Risk Disclosures of Public Companies* (March 2021).[iii]

Turning to the Release itself, we support the consistent disclosure of information in the four main substantive areas covered in the proposed rules according to the Release, namely: material cybersecurity incident and response reporting; cybersecurity risk management policies and procedures; role of management in cybersecurity implementation; and board cybersecurity expertise and oversight. Furthermore, we support use of Inline eXtensible Business Reporting Language (Inline XBRL) for any disclosures as a lever for creating comparability across reporting.

Our work in partnership with our members and with organizations like ISA underscores that the cybersecurity-specific roles of the board and management are distinct. Management holds the power to control and mitigate this risk, and to drill deeply into breaches and

incidents when they happen. The board's role is to make sure that the corporation's cybersecurity program is well managed and that the risk is well controlled.

While we support the overarching goals of these proposed disclosure standards and their alignment with the distinct roles of the board and management, we have suggestions for improvement, clarification, or refinement to meet the reality of board-level cyber-risk oversight. We also urge the commission to review with greater specificity the types of compliance already commonly adopted across organizations before this proposal is completed and enforced.

Many registered companies may already be practicing risk management reporting, adhering to cybersecurity compliance frameworks both voluntary and mandated that could translate to easier reporting against the SEC's proposed rules. (Examples of frameworks follow after our comments on specific questions in the Release.) Still more companies' cybersecurity programs may be too early in their maturity or lacking in funding for the sophistication of reporting requested here. We address these points later in our comment, and hope that the Commission finds these suggestions and comments useful in their final rulemaking.

Answers to the Release's Questions

NACD is pleased to address the questions in the Release that matter to our members who sit on the boards of companies registered with the SEC, including especially provisions that pertain to the role and composition of the board of directors.

Question 5. The Commission asks for comments on a proposed standard that would require prompt disclosure of a cyber breach after the breach is deemed "material," rather than simply after the date of the breach.

> ***NACD's Answer***. Yes, we support the notion that only material breaches should be disclosed, not any and all breaches. Meanwhile, we agree with the discussion of materiality in the Release, which states, citing court cases, that information is material if "there is a substantial likelihood that a reasonable shareholder would consider it important" in making an investment decision, or if it would have "significantly altered the 'total mix' of information made available." This should be up to the company's board and counsel to determine. We would also recommend a reference to materiality standards from the Financial Accounting Standards Board, which is continually fine-tuning the definition of materiality to meet investor needs. Reference to these standards or another that the Commission identifies as most relevant to this form of disclosure would clarify for reporting companies and investors

alike how determinations were made about the materiality of a breach, in whole or in aggregate.

Question 17. The Commission asks whether, in addition to the disclosures already in the proposed rule, there are "other aspects of a registrant's cybersecurity policies and procedures and governance" that should be disclosed.

> ***NACD's Answer***. Yes. One disclosure item that is not in the proposed rule, and which we would recommend, is an affirmative statement that provides assurance to shareholders and other stakeholders that the board plays a role in ensuring adequate company investment in cybersecurity. We also recommend an affirmative statement providing assurance that the board of directors empowers whomever is most senior within the company's cybersecurity program with the resources and reporting lines needed to be a successful business enabler and defender. Finally, we would recommend that the role of internal audit be affirmed as independent when delivering assurance, perhaps periodically in cadence, that cyber risks are well controlled. We would, however, only recommend these points if these assurances could be protected by a safe harbor rule.

Question 23. The Commission asks if the rules for disclosing oversight details should exempt, or at least phase in, smaller companies. (The proposed rules lack such an exemption, on the grounds that smaller companies get attacked with relatively high frequency.)

> ***NACD's Answer***. NACD would support phasing in of the requirement for smaller companies, as long as other safeguards (such as safe harbor and flexibility of definitions) remain in place. In the absence of such safeguards, we would support an absolute exemption for smaller companies. We believe that phasing in should occur because the expertise required will need to be established for some firms to be able to comply with these rules. While there is a national security imperative underlying the Commission's urgency around this rule, other laws have been introduced, voted upon, or passed of late to compel stronger security in smaller businesses—notably the Strengthening American Cybersecurity Act of 2022, which passed in the Senate in March 2022, and the Cyber Incident Reporting for Critical Infrastructure Act of 2022, which became law in March 2022 when the omnibus spending bill was signed into law. We urge this phased in approach to allow smaller companies to focus on maturing their security operations before being beholden to more fulsome reporting to the board and, eventually, to deeper regulation. We also remind the Commission that these smaller organizations may need to place greater attention and emphasis with compliance and reporting on laws meant to defend the homeland—laws that, in many

cases, have tighter time lines for reporting than the SEC's proposed time line of four days from the time of determining that a breach was material.

Question 25. The Commission asks about possible redundancy in its proposed additions to Regulation S-K,[iv] namely a new Item 106 (under Business) to mandate more disclosures about cybersecurity risk management and oversight, including use of auditors,[v] (without mandating a particular framework); and new provisions under Item 407 (under Governance) to mandate disclosure of board expertise in cybersecurity.[vi] The Commission is asking whether these overlap and if so, what to do.

NACD's Answer. This is an important question because Regulation S-K, covering narrative disclosures, together with Regulation S-X, covering numeric disclosures, forms the very basis of the US disclosure framework. Whatever goes into Regulation S-K as a disclosure standard often becomes the operating standard for boards. We appreciate the fact that the SEC is not imposing any particular framework for oversight. *We do not believe that these two areas overlap.* The question of oversight and the question of expertise are different. A strong framework for oversight can make up for the lack of specialized expertise on the board, because outside expertise can be obtained and consulted by the board; however, the converse is not true. The presence of a cybersecurity expert on a board cannot make up for poor oversight processes, and does not excuse the full board from its oversight duties in this matter. We do believe that disclosure about board-level cybersecurity governance should appear in the 10-K, while the disclosure about expertise should appear in the proxy. Furthermore, we believe that these disclosures should appear in the same place in each document. Consistency of placement across documents will facilitate ease of review by interested investors and stakeholders.

Question 27. The Commission asks if companies should be required to disclose the names of persons with cybersecurity expertise on the board of directors.

NACD's Answer. We support identifying by name any directors with cybersecurity expertise (assuming the proposed safe harbor[vii] clause stays), and indeed would expand the disclosure to include statements on any directors who have received education specific to cyber-risk oversight best practices. As written, the proposal may apply only to a narrow margin of directors at registered companies, as only a small portion of directors at publicly traded companies were this type of technologist in their work in management. However, many directors actively seek out ongoing education about cyber-risk oversight best practices and developments related to that duty. This education and experience type is not listed explicitly within the definition of "expertise" within the proposal, and we urge the Commission to expand the

definition of "expertise" to include this education type. The proposed rule makes it clear that responsibility for cyber-risk oversight lies with the full board and not any particular individual, and we strongly support this concept.[viii]

Question 28. The Commission asks if a registrant should be required to disclose the lack of a person with cybersecurity expertise on its board of directors.

> ***NACD's Answer***. We reject this proposed rule. Not every single company will have exposure significant enough to merit the presence of a cybersecurity expert on the board, yet making a disclosure to this effect may act as a false sign of weakness to threat actors that could court trouble for the company. If a company is required to disclose the lack of any role, we propose that they be required to disclose the lack of a designated, management-level role responsible for cybersecurity such as the chief information security officer or equivalent. While board-level oversight may be achieved sufficiently without an expert on the board, a company must be properly staffed and funded, not to mention led by a strong manager, in order to be able to mitigate cyber risks.

Questions 29 through 31. The Commission asks if the mandate to disclose expertise should be accompanied by a required description expertise, or if the current approach of providing a nonexclusive list of examples can work.

> ***NACD's Answer***. We support the currently proposed approach of giving examples, but not requiring any particular type of expertise. Requiring specific types of expertise may lead eventually to specialization of board roles, a move that may undermine board performance and lead to greater financial risk for companies in the long term.

Questions 32 and 33. The Commission asks if disclosure of board expertise should be required in an annual report and proxy or information statement, and if so, where.

> ***NACD's Answer***. We believe that the most important place for the disclosure of director expertise would be the place in the proxy statement where the board is describing qualifications of directors it is proposing for continued board service.

Question 34. The Commission asks if the rules should define "expertise" in the context of board-level cybersecurity qualification.

> ***NACD's Answer***. We do not believe that the Commission should define expertise, but the rules should require companies to do so. For this purpose, the rules could contain an example of how expertise might be defined. Whether the Commission defines

expertise explicitly or provides examples of how companies might define expertise themselves, we urge the Commission to include points made in our response to Question 27 about inclusion of continuing education about board-level cyber-risk oversight best practices.

Question 35. The Commission asks if certain kinds of companies such as smaller companies should be excluded from the requirement to make disclosures about cybersecurity expertise of any particular director/s.

> ***NACD's Answer***. While we support exemptions in other areas, we do not believe that it is necessary to exempt smaller companies from the cybersecurity expertise disclosure, provided that all other related aspects of the rules remain intact, as discussed above in Questions 28 (re a safe harbor) and 28–31 (re definitions).

Question 36. The Commission asks if commenters support the proposed safe harbor, which clarifies that a director identified as having expertise in cybersecurity would not have any increased level of liability under federal securities laws.

> ***NACD's Answer***. We strongly support this provision in the proposed rules and would recommend in addition a safe harbor for descriptions of oversight.

Suggestion for Creating Efficiencies
As stated above, we would like to offer some concepts for the Commission to consider ahead of finalizing this rule.

- **Review commonly used risk management frameworks and align SEC disclosure rules to drive efficiency.** Registered companies with mature cybersecurity risk management practices are already complying with a litany of laws and industry-relevant compliance frameworks both voluntary and mandated in nature. NACD and ISA in its handbook suggest that companies of all types at minimum measure risk over time against the National Institute of Standards and Technology's Cybersecurity Framework (NIST-CF). NIST-CF is widely used and translates complex cybersecurity risk concepts into terminology and reports that are well understood by corporate board members.

  The economic analysis of the Release acknowledges that many companies are beholden by law to use NIST-CF, and those companies may be layering other voluntary and mandatory compliance frameworks on top of or alongside it. Some popular examples of other frameworks include the International Organization for Standardization (ISO)'s Standards 27001 and 27002, and Service Organization Control

Type 2 (SOC 2), which was developed by the AICPA. There are a number of other compliance frameworks that stakeholders in registered companies are demanding be in place in order to do business with those companies, and many already account for cybersecurity corporate governance—especially SOC 2.[ix]

Given current rigor around compliance with best practices and these frameworks, we urge the Commission and its staff to provide guidance on how companies can map current compliance disclosures in these frameworks back to the SEC's desired uniformity of disclosure. This would create efficiencies for companies already doing due diligence and provide a road map for boards looking to advise and nurture strong oversight practices and reporting.

- **Balance the need for consistently reported information with the demands of securing a company and empowering innovation.** We also believe that aligning SEC disclosure with compliance measures already in place would empower companies to build security into their products and innovation efforts. Enabling cybersecurity practitioners to focus on those two business areas would create value for shareholders, instead of demanding further time and investment into compliance work that might already be happening in one or more other places.

  Managers of mature security teams are already spending an outsized amount of time meeting compliance requirements, a task that pulls their attention away from the time-sensitive and complex nature of detecting and responding to security incidents—not to mention building a culture of security and innovation within their companies. It might also distract security leaders from reporting clearly to the board on the risks that the company faces and lead to the security organization being underfunded.

  According to a 2021 survey of global chief information security officers (CISOs) conducted by EY,[x] one in two surveyed CISOs note that ensuring compliance can be the most stressful part of their jobs. One CISO interviewed—of a major social media platform—noted that he spends between 50 to 60 percent of his time on regulatory matters. Meanwhile, where compliance once was a tool for CISOs to make the case to their boards that the security organization required more fulsome funding, this 2021 survey found that only 18 percent of respondents saw compliance as a way to acquire sufficient budget—down from 29 percent in the 2020 survey by the same firm.

  To draw a line under this point, it would be prudent to streamline the regulatory demands of this Release with the processes already in place in other state, local, and federal agencies in order to empower the CISO to create a culture of security that supports innovation.

Empowering Directors. Transforming Boards.

In conclusion, we support the proposed rules in general, hope that our comments and suggestions for improvements are of value to the Commission as it considers its final rulemaking, and encourage the Commission to retain and expand upon the safe harbor provisions already stated in the Release.

As Chair Gensler reminded us recently, cybersecurity is a team sport. We are all in this together.

Sincerely,

Peter R. Gleason, President and CEO
William McCracken, Chair
National Association of Corporate Directors
Arlington, VA

APPENDIX:
Five Principles for Cyber-Risk Oversight
(From *Cyber-Risk Oversight 2020, Key Principles and Practical Guidance for Corporate Boards*, NACD: 2020)

Principle 1: Cybersecurity as a Strategic Risk. Directors need to understand and approach cybersecurity as a strategic, enterprise risk—not just as an IT risk.

Principle 2: Legal and Disclosure Implications. Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.

Principle 3. Board Oversight Structure and Access to Expertise. Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on board meeting agendas.

Principle 4. Enterprise Framework for Managing Cyber Risk. Directors should set the expectation that management will establish an enterprise-wide, cyber-risk management framework with adequate staffing and budget.

Principle 5. Cybersecurity Measurement and Reporting. Board-management discussions about cyber risk should include identification and quantification of financial exposure to cyber risks and which risks to accept, mitigate, or transfer, such as through insurance, as well as specific plans associated with each approach.

Empowering Directors. Transforming Boards.

[i] The Release is available at this URL: https://www.sec.gov/rules/proposed/2022/33-11038.pdf.
[ii] NACD, *Cyber-Risk Oversight 2020* (Arlington, VA: NACD, 2020).
[iii] SecurityScorecard, NACD, Cyber Threat Alliance, IHS Markit, and Diligent, *The State of Cyber-Risk Disclosures of Public Companies* (2021).
[iv] The full question is as follows: "25. To what extent would disclosure under proposed Item 106 overlap with disclosure required under Item 407(h) of Regulation S-K ("Board leadership structure and role in oversight") with respect to board oversight of cybersecurity risks? To the extent there is significant overlap, should we expressly provide for the use of hyperlinks or cross-references in Item 106? Are there other approaches that would effectively decrease duplicative disclosure without being cumbersome for investors?"
[v] "We are also proposing to add new Item 106 of Regulation S-K that would require a registrant to: (1) provide updated disclosure in periodic reports about previously reported cybersecurity incidents; (2) describe its policies and procedures, if any, for the identification and management of risks from cybersecurity threats, including whether the registrant considers cybersecurity risks as part of its business strategy, financial planning, and capital allocation; and (3) require disclosure about the board's oversight of cybersecurity risk, management's role in assessing and managing such risk, management's cybersecurity expertise, and management's role in implementing the registrant's cybersecurity policies, procedures, and strategies."
[vi] "We also are proposing to amend Item 407 of Regulation SK to require disclosure of whether any member of the registrant's board has expertise in cybersecurity, and if so, the nature of such expertise."
[vii] "Proposed Item 407(j)(2) would state that a person who is determined to have expertise in cybersecurity will not be deemed an expert for any purpose, including, without limitation, for purposes of Section 11 of the Securities Act (15 U.S.C. 77k), as a result of being designated or identified as a director with expertise in cybersecurity pursuant to proposed Item 407(j). This proposed safe harbor is intended to clarify that Item 407(j) would not impose on such person any duties, obligations, or liability that are greater than the duties, obligations, and liability imposed on such person as a member of the board of directors in the absence of such designation or identification. This provision should alleviate such concerns for cybersecurity experts considering board service. Conversely, we do not intend for the identification of a cybersecurity expert on the board to decrease the duties and obligations or liability of other board members."
[viii] "Conversely, we do not intend for the identification of a cybersecurity expert on the board to decrease the duties and obligations or liability of other board members."
[ix] For more information on the SOC 2 report, visit this webpage: https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.
[x] See "Cybersecurity: How do you rise above the waves of a perfect storm?," posted on ey.com on July 22, 2021, and available at this URL: https://www.ey.com/en_us/cybersecurity/cybersecurity-how-do-you-rise-above-the-waves-of-a-perfect-storm#Chapter2