Statement

Dissenting Statement on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Proposal

Commissioner Hester M. Peirce

March 9, 2022

Thank you, Renee, Ian, and Jessica. Cybersecurity risk is top of mind for everyone. The Commission's consideration of this topic—whether for investment advisers, as we did a month ago,[1] or public companies, as we are doing today—is, therefore, reasonable. We must approach this topic, of course, through the prism of our mission. We have an important role to play in ensuring that investors get the information they need to understand issuers' cybersecurity risks if they are material. This proposal, however, flirts with casting us as the nation's cybersecurity command center, a role Congress did not give us. Accordingly, I respectfully dissent.

Our role with respect to public companies' activities, cybersecurity or otherwise, is limited. The Commission regulates public companies' disclosures; it does not regulate public companies' activities. Companies register the offer and sale, and classes of securities with the Commission; they themselves are not registered with us, and we do not have the same authority over public companies as we do over investment advisers, broker-dealers, or other registered entities.

The proposal, although couched in standard disclosure language, guides companies in substantive, if somewhat subtle, ways. First, the governance disclosure requirements embody an unprecedented micromanagement by the Commission of the composition and functioning of both the boards of directors and management of public companies. First, the proposal requires issuers to disclose the name of any board member who has cybersecurity expertise and as much detail as necessary to fully describe the nature of the expertise. Second, the proposal requires issuers to disclose whether they have a chief information security officer, her relevant expertise, and where she fits in the organizational chart. Third, the proposal requires granular disclosures about the interactions of management and the board of directors on cybersecurity, including the frequency with which the board considers the topic and the frequency with which the relevant experts from the board and management discuss the topic.

Such precise disclosure requirements look more like a list of expectations about what issuers' cybersecurity programs should look like and how they should operate. The closest analogue is the Sarbanes-Oxley Act disclosure requirement relating to audit committee financial experts.[2] Congress mandated that foray into corporate governance, which, at least, was directly related to the reliability of the financial statements at the heart of our disclosure system. We are going a step further this time by requiring detailed disclosure about discrete

subject matter expertise of directors and employees who are not necessarily executive officers or significant employees, and about the frequency of interactions between the board and management on a specific topic.

While the integration of cybersecurity expertise into corporate decision-making likely is a prudent business decision for nearly all companies, whether, how, and when to do so should be left to business—not SEC—judgment.[3] Regulators may have a role to play in working with companies on cybersecurity, but we are not the regulators with the necessary expertise.

The proposed rules also require companies to disclose their policies and procedures, if they exist, for the identification and management of risks from cybersecurity threats. Again, while cloaked as a disclosure requirement, the proposed rules pressure companies to consider adapting their existing policies and procedures to conform to the Commission's preferred approach, embodied in eight specific disclosure items. The enumerated disclosure topics likely make sense for many public companies, but securities regulators are not best suited to design cybersecurity programs to be effective for all companies, in all industries, across time. The proposal's detailed disclosure obligations on these topics will have the undeniable effect of incentivizing companies to take specific actions to avoid appearing as if they do not take cybersecurity as seriously as other companies. The substance of how a company manages its cybersecurity risk, however, is best left to the company's management to figure out in view of its specific challenges, subject to the checks and balances provided by the board of directors and shareholders.

The proposal's bright spot is the rules relating to the reporting of cybersecurity incidents. I am not convinced that the rules are necessary in light of the Commission's 2018 guidance,[4] which provided our views about public companies' disclosure obligations under existing rules. Nevertheless, the proposed rules seem to provide sensible guideposts for companies to follow in reporting material cybersecurity incidents. Properly rooted in materiality, these proposed rules afford companies the necessary flexibility to get their arms around the magnitude of a cybersecurity incident before the four-day disclosure clock begins to run. I look forward to reading commenters' reactions to whether we have structured a workable incident reporting framework.

My primary concern with the proposed incident reporting requirements is that we are unduly dismissive of the need to cooperate with, and sometimes defer to, our partners across the federal government and state government. For example, if delaying disclosure about a material cybersecurity incident could increase the chances of recovery of stolen funds or the detection of the wrongdoers in the expert opinion of law enforcement agencies, we should consider whether temporary relief from our disclosure requirements would best protect investors. The tension between ensuring that investors get material cybersecurity incident information and protecting the ability of law enforcement to pursue wrongdoers is difficult to resolve appropriately, and I look forward to hearing how commenters would resolve it.

Thank you to the staff in, among others, the Division of Corporation Finance, the Division of Economic and Risk Analysis, and the Office of General Counsel for your evident and unrelenting hard work in preparing this release and for the considerable time you spent with me in response to my questions and concerns. I look forward to reviewing commenters' thoughts on the proposal.

---

[1] *See* Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, Rel. No. 33-11028 (Feb. 9, 2022), *available at* https://www.sec.gov/rules/proposed/2022/33-11028.pdf. *See also* Commissioner Hester M. Peirce, *Statement on Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies* (Feb. 9, 2022), *available at* https://www.sec.gov/news/statement/peirce-statement-cybersecurity-risk-management-020922.

[2] Sarbanes-Oxley Act of 2002 § 407, 15 U.S.C. 7265 (2018).

[3] If adopted, today's rule likely will increase the already high demand for cybersecurity experts, which, ironically, may make it harder for companies to get the help they need.

[4] Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Rel. No. 33-10459 (Feb. 26, 2018) [83 FR 8166], *available at* https://www.sec.gov/rules/interp/2018/33-10459.pdf.