SOCIETY
for Corporate Governance

August 5, 2022

Vanessa A. Countryman
Secretary
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, D.C. 20549–1090

RE: Supplemental Comment Letter on Proposed Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, SEC File Number S7–09–22

Dear Ms. Countryman:

The Society for Corporate Governance ("Society") submits this letter in response to the request for public comments by the Securities and Exchange Commission ("SEC" or the "Commission") on the proposed rulemaking, "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," ("Proposed Rule") as announced by the Commission on March 9, 2022, and published in the Federal Register on March 23, 2022, at 87 FR 16590, File Number S7-09-22. Founded in 1946, the Society is a professional membership association of more than 3,600 corporate and assistant secretaries, in-house counsel, outside counsel, and other governance professionals who serve approximately 1,600 entities, including 1,000 public companies of almost every size and industry.

This letter, which supplements our comment letter dated May 9, 2022,[1] follows a meeting between members of the Society's Securities Law Committee and representatives of the staff of the SEC's Division of Corporation Finance on June 2, 2022. In particular, this letter responds to the staff's expression of interest in receiving empirical information on investor requests for cybersecurity information from companies as well as potential alternatives to the proposed Form 8-K incident disclosure requirement. We appreciate the Commission's attention to this additional commentary.

[1] Society for Corporate Governance, Comment Letter on Proposed Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (May 9, 2022).

I. Society Survey Reveals That Few Investors Request Cybersecurity Details from Companies

A. Investors Do Not Seek Granular Details Required by Proposed Rule

As Society members expressed to staff in the June meeting, institutional investors do not seek the granularity of information from companies that the Proposed Rule would require. In a recent survey of the Society's issuer members,[2] only around 10-20% of the 192 respondents reported that their shareholders have requested information or asked a question on the following cybersecurity-related information:

- The process by which the board is informed about cybersecurity risks (20.3%)
- Whether and how the board or committee considers cybersecurity risks as part of its business strategy, risk management, or financial oversight (18.9%)
- Activities the company takes to prevent, detect, or minimize effects of cybersecurity incidents (17.5%)
- The frequency of the board's discussion of cybersecurity risks (15.4%)
- Information about the directors' experience in cybersecurity (14.3%)
- A description of the company's cybersecurity risk assessment program (11.2%)
- Information about the specific management positions or committees responsible for cybersecurity risk (10.5%)
- How cybersecurity risks are considered as part of business strategy, financial planning, and capital allocation (8.4%)
- A description of the company's policies and procedures for identification and management of risks from cybersecurity threats (7%)
- Policies and procedures to oversee and identify cybersecurity risks associated with the use of any third-party service provider (4.2%)

[2] Society for Corporate Governance, *Survey: Cybersecurity: Investor Priorities* (June-July 2022) (on file with author). Respondent demographics consisted of 56.3% mega and large-cap issuers ($10 billion or larger market cap); 31.3% mid-caps ($2 billion to $10 billion in market cap); and 12.5% small- and micro-caps (less than $2 billion). The companies spanned a wide variety of industries, with the top six sectors represented being Manufacturing – Industrial (11.3%), Banking/Finance (14.6%), Energy (7%), Retail/Wholesale (8.1%), Healthcare/Pharma (5.4%), and Technology (13%). The survey generated 192 responses over a four-week period in June and July 2022.

- The process by which management personnel are informed about cybersecurity risks (4.2%)
- The use of assessors, consultants, auditors, or other third parties in connection with any cybersecurity risk assessment program (3.5%)
- Information about the company's chief information security officer, or the equivalent (3.7%)
- How previous cybersecurity incidents have informed changes in governance, policies and procedures, or technologies (1.4%)
- The existence of previously undisclosed individually immaterial incidents that, if aggregated, would be material (0.0%).

Overall, 64.3% of the respondents indicated that their investors had not engaged with them on any of the listed topics.

The survey results indicate that, even for the minority of companies engaged by their shareholders on these topics, investors have not requested the granularity of disclosures that would be required under the Proposed Rule. Requests for detailed information regarding the board's oversight, including its role in overseeing the management of cybersecurity risks, along the lines contemplated by the Proposed Rule, are anomalous. As one respondent described their company's experience:

> *Investors don't typically ask questions that specifically – they ask generally about how the board oversees cybersecurity risk, and generally how management handles cybersecurity risk management – some conversations may go to third-party assessment (both third parties used to do our internal assessments, and our assessment of third-party risk). That additional level of detail is very rare – the questions are much more high-level and focused on whether the board is "paying attention" to cybersecurity risk as part of the suite of risks it oversees.*

The Commission's 2018 cybersecurity guidance already provides that, for companies where cybersecurity risk is material, Item 407(h) of Regulation S-K and Item 7 of Schedule 14A regarding board oversight of risk should include a description of the board's management of cybersecurity risk. Based on our member input, bolstered by these recent survey results, we believe that the existing Item 407(h) of Regulation S-K and Item 7 of Schedule 14A are sufficient to elicit the desired disclosure.

If the SEC nevertheless pursues additional disclosure requirements, we request that in lieu of the detailed, prescriptive requirements proposed, the final rule be modified to a include a list of categories for disclosure. For example, the SEC could amend the current risk and governance disclosure requirements in Regulation S-K to add language to indicate that cyber-

related information must be disclosed. Specifically, the SEC could amend Item 407(h) to expressly require disclosure of the board of directors' oversight of cybersecurity-related risk.

Also noteworthy is that our 192 survey respondents reported that *no investors requested information* about aggregated incidents, an aspect of the Proposed Rule that our initial letter noted would be difficult for issuers to understand and implement, and of limited value to investors.

B. Respondents Express Concerns About Proposed Incident Disclosure

We also surveyed members about the nature of their concerns with the proposed Form 8-K incident disclosure requirement. While the four-day deadline for reporting cyber incidents would be triggered by a materiality determination by the company, our initial letter noted the many challenges that companies would face in making these subjective assessments in rapidly evolving situations. Given these difficulties and companies' concerns about later legal and regulatory actions challenging the timing of their disclosures, we expect that many companies will opt to make placeholder or boilerplate disclosures before knowing the full details about a cybersecurity incident or whether it is actually material.[3] As a result, investors likely will be overloaded with excessive, unhelpful, and potentially confusing disclosures and may overlook those disclosures about material incidents, as some have noted.[4] Such premature disclosures may lead investors (especially retail shareholders who have less access to corporate officials) to make ill-advised decisions to sell their shares based on incomplete information. In these ways, the proposed Form 8-K requirement has the potential to undermine the Commission's mission to protect investors.

---

[3] In its comment letter, the American Investment Council, which represents private equity firms, likewise warned that issuers may feel compelled by the proposed incident reporting requirement to make many placeholder filings that are not useful for investors. *See* American Investment Council, Letter re: Four Business Day Cybersecurity Incident Reporting Requirement under the Proposed Amendment adding Item 1.05 to Form 8-K pursuant to the Securities Exchange Act of 1934 (May 9, 2022) ("The Proposed Item incentivizes issuers to file 'placeholder' disclosures that contain information that is vague or likely to change, in order to avoid any doubt that they have met the four business-day notification requirement. The resulting flood of ambiguous and equivocal disclosures (which will include notifications for cybersecurity incidents that ultimately turn out not to be material) will undermine the SEC's investor protection mission because investors will not be able to identify the information that actually matters to their investments. Indeed, given the likely volume of 8-Ks that will be of limited value, investors may become numb to these disclosures – which would undercut the SEC's stated purpose of equipping investors and market participants with information to 'assess the possible effects of a material cybersecurity incident' on an issuer.").

[4] Asset manager Federated Hermes raised similar concerns about investor confusion in its comment letter. *See* Comment Letter of Federated Hermes, Inc. on the Securities and Exchange Commission's Proposed Cybersecurity Rules for Public Companies (May 9, 2022) ("This subjective 'materiality' standard, coupled with a potentially impending filing deadline in order to comply with the four (4) business day disclosure requirement, will result in registrants over-reporting cybersecurity incidents, which may lead to investors undervaluing cybersecurity incident disclosures . . . . Although the timeframe for filing is conditioned on the registrant's 'determination' that a material event has occurred, the requirement as drafted would likely facilitate early disclosure of events which may eventually turn out to be immaterial, resulting in overdisclosure and potential investor confusion.").

Of the 137 respondents who answered this Society survey question, only eight indicated they did *not* believe that Form 8-K's four-business day deadline for reporting incidents would be impractical for the company or potentially harmful to companies and investors; five were uncertain. The overwhelming majority – 90.5% – expressed concerns about practicality and/or harm to companies, investors, and/or law enforcement.[5]

Our survey also asked our issuer members to elaborate about their concerns over the impact of the Proposed Rule's incident reporting requirement. Respondents provided the following commentary, highlighting the potential harm that premature public disclosure of an ongoing incident can cause:

- *Publicly disclosing an unremediated vulnerability publicly is asking to become the target of additional attacks while the company is properly focused on remediating the issue as quickly as possible. It exponentially raises the risk for the company, which, in turn, is harmful to investors.*
- *Both impractical and potentially harmful; it draws critical focus from management's need to access and remediate.*
- *Premature disclosure could be harmful to the company if it serves only to exacerbate the impact of the incident.*
- *In addition to compromising negotiations with criminals, too much may be unknown at that time, resulting in misleading or meaninglessly vague disclosure.*
- *It would potentially put the company at odds with law enforcement and our ability to understand the problem.*
- *Potentially harmful to everyone except the cyber criminals.*

Respondents also noted the difficulty of understanding the scope and magnitude of an evolving incident; the need for adequate time for the company to assess the scope, magnitude, and impacts of the incident; the potential harms associated with premature disclosure; and the inevitability of post-event second-guesting by regulators and an active plaintiffs' bar. As one respondent explained, the proposed incident reporting would be impractical while providing limited benefits to investors:

It's impractical because facts are developing quickly and there is potential for incorrect

[5] The concerns expressed by our members about the proposed incident reporting requirements are consistent with those expressed by other industry advocates. In a comment letter signed by 35 industry associations, the U.S. Chamber of Commerce asked the SEC to revise the Proposed Rule to allow for temporary delays in public disclosure. *See* U.S. Chamber of Commerce et. al, Comment Letter on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (June 22, 2022) ("Instead of undercutting industry-government cooperation, the SEC should urge companies to work with law enforcement and national security agencies to mitigate the impacts of cyber incidents and help bolster companies' security and financial positions, which would benefit investors.").

conclusions while investigations are underway. While tying it to materiality gives appropriate flexibility, the focus on promptness combined with the 4-day business clock runs the risk of market volatility due to incomplete or potentially inaccurate information based on the ongoing nature of the investigation. Further, even if a company knows an event is material, the unknown information creates unnecessary market volatility with little benefit. Are investors really being protected if what they get from the rule is incomplete or potentially inaccurate information, accompanied by market volatility?

II. Potential Alternatives to the Proposed Incident Disclosure Requirement

In our May 9 letter, we expressed multiple concerns about the Commission's proposed approach to incident reporting via Form 8-K – most notably, that the premature public disclosure of incidents that have not been substantially remediated, or that are the focus of law enforcement or national security activities, will cause harm to companies and their investors. To alleviate these concerns, in lieu of the proposed Form 8-K trigger, we suggested that disclosure of cyber incidents be based on the following priorities:

(1) an expedient disclosure, without unreasonable delay;
(2) allow for a delay in public disclosure when requested by law enforcement or government agencies focused on national security or the security of critical infrastructure;
(3) allow for measures necessary to determine the scope of the breach and restore the reasonable integrity of the impacted system(s) or data prior to public disclosure, and;
(4) allow for reasonable notification to individuals with impacted data.

As we noted in our May 9 letter, these considerations better reflect the interests and priorities that issuers should consider when evaluating the timing and content of public disclosures of cybersecurity incidents. These criteria would allow issuers to weigh the factors associated with complex situations and the risks of premature disclosure and to make disclosure decisions in accordance with reasonable judgments around those potentially competing interests and goals.

During our June 2 meeting, the Commission staff suggested that they would have difficulty learning about national security concerns, law enforcement investigations, or other reasons for delaying public disclosure of cyber incidents and would thereby be hampered in their enforcement efforts if they were to disagree with a company's disclosure judgment.

First, and most importantly, we do not think this concern is serious enough to justify exposing companies, investors, and others to meaningful harm from premature disclosure. The Commission does not ordinarily have contemporaneous information about any company's

decision *not* to disclose a particular fact. Rather, the SEC relies on its traditional investigation (such as staff comment letters) and enforcement tools to gather information and assign consequences to improper decisions not to disclose after the fact; this system has been in place for decades and has proven effective.[6] Those same investigation and enforcement tools would be available to gather information from a company about its disclosure decision-making process and determine whether it had improperly delayed public disclosure; there is no principled reason that these measures would not be effective in this context.[7] Companies that choose to delay the public disclosure of incidents that would otherwise be material will carefully document their decision-making process in anticipation of this scrutiny, and companies will not make decisions to delay disclosure lightly.

As noted earlier, we expect that most companies will probably err on the side of over-disclosing marginally material incidents and/or providing limited details, but there will be some incidents where the risk of harm to the company, its customers, or law enforcement or national security interests will be so great that a delay in public disclosure will be necessary. Given that most major cybersecurity incidents impact more than one company, the risk that the Commission will never learn about material incidents is extremely small.

If the Commission continues to have concerns about obtaining information on emerging cybersecurity incidents, the Society suggests an alternative, whereby issuers would confidentially notify the Commission staff of their decision to delay disclosure of an otherwise material incident due to concerns about additional damage from an incident that has not been substantially remediated, or to protect the interests of law enforcement, national security, or the security of critical infrastructure. The Commission's question in the Proposed Rule about whether a delay in disclosure should be allowed where the Attorney General makes a written request to the Commission for national security reasons (page 30) demonstrates that the Commission has the authority to allow delayed public disclosure to avoid further harm. There are existing mechanisms by which the Commission could be confidentially informed by an issuer of a material incident that would otherwise be subject to public disclosure.[8] In such a communication

---

[6] *See, e.g.*, "Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees to Pay $35 Million," SEC News Release 2018-71 (April 24, 2018) (Director of Enforcement: "We do not second-guess good faith exercises of judgment about cyber-incident disclosure. But we have also cautioned that a company's response to such an event could be so lacking that an enforcement action would be warranted.").

[7] *See generally In the Matter of Altaba Inc., f/d/b/a Yahoo! Inc.,* SEC Release No. 3927, 2018 WL 1919547 (April 24, 2018) (finding Yahoo's senior management and legal staff did not properly assess the scope, business impact, or legal implications of the data breach, including how it should have been disclosed in public filings); *In re First American Fin. Corp.*, SEC Release No. 92176 (June 14, 2021) (the SEC concluded that a company violated internal controls requirements by failing to alert senior officers to system vulnerability for several months).

[8] The Commission staff routinely receives confidential treatment requests from market participants who wish to delay public disclosure. One example is the Commission's process for reviewing confidential treatment requests from investment managers who wish to delay disclosing certain positions in their quarterly 13F filings. In our view,

to the SEC (which could be via telephone[9] or a confidential filing), issuers could provide a brief description of the incident, the company's reasons for delaying disclosure (such as a request from law enforcement), and the company's expectation regarding when it could make a public filing to disclose the incident. The Commission staff could then, if appropriate, engage in communication with the issuer about its disclosure decision, with the goal of reaching a mutual understanding about the most appropriate timing for disclosure. Confidential engagement between companies and the SEC staff would reduce the likelihood that premature public disclosure would harm a company's investors or customers and/or jeopardize critical infrastructure or the interests of law enforcement or national security.[10]

While the Society believes that such a confidential contemporaneous notification would be unnecessary in light of the Commission's traditional investigation and enforcement tools, we also believe that allowing companies to delay public disclosure to avoid further harm to investors, customers, critical infrastructure, or national security/law enforcement interests is a very important priority that clearly outweighs the need for investors to learn immediately about emerging or unremedied cybersecurity incidents.

Thank you for considering the Society's additional views on cybersecurity disclosure.

---

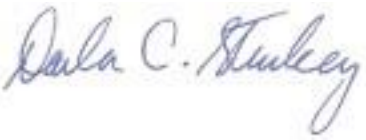
companies would have more compelling reasons, such as national security, a pending law enforcement investigation, or exacerbating harm to customers or shareholders, to delay public disclosure, than the purely pecuniary reasons that motivate 13F filers to request confidential treatment. Further evidence of the feasibility of confidential reporting can be found in the Commission's recently proposed rule on short sale disclosure. Proposed Rule 13f-2 would require investment managers to confidentially file a Form SHO with the SEC within 14 calendar days after the end of each calendar month. *See* Fact Sheet: Enhancing Short Sale Disclosure (Feb. 25, 2022), https://www.sec.gov/files/34-94314-fact-sheet.pdf.

[9] In its comment letter, Federated Hermes suggested a similar confidential reporting mechanism for cybersecurity incidents. Supra note 4. ("A regime that required telephonic notification to the Commission of a potential material event, coupled with a requirement to file an 8-K at the resolution of a determined material event, would, in our view, be a better approach.").

[10] In a speech on cybersecurity in April 2022, Chair Gary Gensler acknowledged the importance of national security, coordination with federal cybersecurity agencies, and other considerations beyond public disclosure. "Given the SEC's mission, and the evolving cybersecurity risk landscape, when considering work at the SEC, I think about it in three ways: cyber hygiene and preparedness; cyber incident reporting to the government; and in certain circumstances, disclosure to the public." *See* Chair Gensler, "Working On 'Team Cyber' -- Remarks Before the Joint Meeting of the Financial and Banking Information Infrastructure Committee and the Financial Services Sector Coordinating Council" (April 14, 2022). Chair Gensler's remarks suggest that it would be appropriate to temporarily delay public disclosure to protect national security/law enforcement interests or to prevent further harm to consumers.

Respectfully submitted,

Ted Allen
Vice President, Policy & Advocacy
Society for Corporate Governance



Darla Stuckey
President and CEO
Society for Corporate Governance

cc: Chair Gary Gensler
Commissioner Hester Peirce
Commissioner Caroline Crenshaw
Commissioner Mark Uyeda
Commissioner Jaime Lizárraga
Renee Jones, Director, Division of Corporation Finance
Erik Gerding, Deputy Director, Division of Corporation Finance