WILSON SONSINI

Wilson Sonsini Goodrich & Rosati
Professional Corporation
650 Page Mill Road
Palo Alto, California 94304-1050
[redacted]

May 9, 2022

Via Electronic Delivery

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

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

Dear Ms. Countryman:

We appreciate the opportunity to comment on the U.S. Securities and Exchange Commission ("Commission") proposed rules to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and cybersecurity incident reporting by public companies (the "Cybersecurity Reporting Proposal").

Our firm is the premier provider of legal services to technology, life sciences, and growth enterprises worldwide. We represent over 300 public companies and have represented over 300 issuers in initial public offerings since 1998. We regularly advise public companies and their officers and directors regarding cybersecurity oversight and governance, as well as the response to and disclosure of security incidents. We recognize cybersecurity is important, increasingly discussed in the boardroom, and further guidance from the Commission is helpful and welcome. We generally support the Commission's efforts to improve the consistency, quality and timeliness of disclosure related to cybersecurity governance, risk management, and incidents; however, we believe that certain aspects of the Cybersecurity Reporting Proposal are problematic, could harm companies experiencing an incident, their shareholders or others, and could undermine law enforcement investigations and companies' cybersecurity programs.

Comments Regarding Proposed Disclosure of Cybersecurity Incidents on Form 8-K

We support the proposal that the trigger for notification should be the determination of a material cybersecurity incident.

The Commission is proposing to amend Form 8-K to add a new Item 1.05 that would require disclosure of specific information about a material cybersecurity incident. We agree with the Commission's determination that the trigger for an Item 1.05 Form 8-K should be from the date on which a cybersecurity incident is determined to be material. Investigations of cybersecurity incidents often do not follow a linear path, and new findings and developments are often identified as the investigation unfolds. When companies

are first alerted to a potential cybersecurity incident, the scope and extent of the incident often are not immediately obvious, and it can take time to investigate and determine whether a cybersecurity incident could have a material impact on the company. As such, we support the Commission's proposal that the trigger for an Item 1.05 Form 8-K should be the date on which the cybersecurity incident is determined to be material.

We believe that proposed Item 1.05 should permit reporting delays, such as where disclosure could disproportionately harm the company and its shareholders.

The Commission recognizes that many state laws permit delayed reporting incidents at the request of and in support of law enforcement investigations, but ultimately rejects reporting delays for purposes of not interfering with ongoing law enforcement investigations even when doing so may hinder law enforcement efforts. However, the Commission does not consider whether the disclosure of an ongoing incident prior to remediation could cause further harm to the company and its shareholders.

In cases of nation-state actors or other advanced persistent threats (APTs)-- one of the most significant threats to U.S. companies–it is unlikely that a company will successfully and comprehensively isolate and eject such attackers from its systems prior to determining the materiality of the incident or within four days after that determination. These sophisticated attackers may have the resources to create multiple points of entry to a company's network and move laterally across systems. By creating multiple means of access, such attackers can build persistence, such that if one point of access is cut off, the attacker can return through another method. Alerting the attacker to the company's knowledge that the attacker is in the company's systems can result in the attacker ceasing activity but leaving multiple backdoor points of access, so that the attacker can easily return when an investigation has ceased.

When conducting an investigation of sophisticated attackers, such as an APT attack, industry-standard advice of leading forensic companies is for companies to avoid using corporate communications to discuss the discovery of the attacker because many APTs monitor corporate communications to ensure that they continue to operate unnoticed. Requiring companies to disclose the discovery of a material APT attack prior to ensuring the attack has been contained and remediated could cause further material harm to the company, requiring board members to choose between their reporting obligations and their fiduciary duties to shareholders.

In addition, by tipping off an attacker that a company is aware that the attacker is in the company's systems, an attacker can react in a manner that harms individuals. In the case of ransomware attacks, many attackers steal data before encrypting the company's systems and data, threatening to post the data on the dark web, if the affected company does not pay a ransom. Even companies that have no intention of paying a ransom may desire to inform affected individuals and offer such individuals identity theft protection services before the stolen data is posted on the dark web. Having only four days after determining that a cybersecurity incident is material may be insufficient time to review stolen data to determine who is affected, procure identity protection services, and provide notice to affected individuals. Hindering the company's ability to mitigate potential harm to affected individuals could exacerbate the potential exposure to the company, which in turn, could cause further material reputational and other types of harm to the company and its shareholders.

Furthermore, a company may have to disclose a cybersecurity incident that still has active vulnerabilities, which could exacerbate the severity of the incident as other potential attackers could become aware of such vulnerabilities and try to exploit them.

We believe that rushed disclosure may impact the completeness and accuracy of the disclosure.

In addition, there is a risk that disclosures that are rushed may be too broad and generic or, even more problematic, incomplete, inaccurate and potentially misleading. In his statement supporting the Cybersecurity Reporting Proposal, Chair Gensler stated, "When companies have an obligation to disclose material information to investors, they must be complete and accurate. Their disclosures also should be timely." However, it is often the case that an investigation uncovers new findings as the investigation develops. If there are disclosure obligations before facts are fully understood, a company may run the risk of making statements that quickly turn out to be inaccurate, or, out of fear of making an inaccurate statement, may not provide disclosures that are as fulsome or helpful to investors as the company would otherwise make after having some time to investigate and obtain a more complete understanding of the incident.

We suggest that companies, with the option to consult with government agencies with deep cybersecurity experience, as helpful, be the appropriate decisionmakers on the propriety of delayed disclosure.

The Commission's request for comments on the Cybersecurity Reporting Proposal suggests that the Attorney General could be granted authority to delay disclosure. The Attorney General is not the appropriate entity to make this determination for two reasons: (1) s/he is not in the best position to determine the best interests of the company or its shareholders, and could be motivated by other interests, and (2) the Department of Justice is not the primary, or even the lead, organization in the federal government for cybersecurity response, rather the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency is often the first call that companies make, and it has independent authorities. For defense contractors, the Department of Defense is likely to have the highest interest in the timing of an announcement.

Ultimately, however, the board of directors is best suited to determine whether a delayed disclosure is in the best interests of the company, and the Commission should empower the board of directors to decide whether additional guidance from government agencies would be helpful. If the Commission decides the involvement of a government agency is prudent, we recommend that the Commission take an approach similar to the Department of Treasury's Office of Foreign Assets Control's (OFAC) approach to ransomware payments. Similar to how OFAC considers a company's report of a ransomware attack to law enforcement to be a significant mitigating factor in determining enforcement outcomes if a ransomware payment is determined to have a sanctions nexus, we recommend the Commission consider a company's consultation with government agencies as a significant factor in support of the propriety of the delayed disclosure.

If the Commission proceeds with requiring the Form 8-K disclosure within four business days of determining a cybersecurity incident is material, the Commission should allow board members to decide to delay reporting if doing so could cause material harm to the company. If the board of directors makes such a delay, it should also articulate why the board of directors decided to delay disclosure of the incident.

Comments Regarding Proposed Disclosure Regarding the Board of Directors' Cybersecurity Expertise

We believe that risk should be managed by the board of directors at the enterprise level, rather than prioritizing cybersecurity expertise over other areas of expertise.

We agree with the Commission that cybersecurity is a top priority of many boards of directors, as we frequently advise on such risks with board members of our clients. However, board members are expected to manage a wide range of risks that companies face, from cybersecurity risk to geopolitical risks to climate risks to regulatory and litigation risks. Aside from financial expertise, the Commission does not require companies to disclose board members who have specialized expertise in other areas of risk management. Requiring disclosure of cybersecurity expertise distinguishes cybersecurity as though it is a risk that should be managed differently and not within a broader understanding of enterprise risk management. This approach goes against established guidance to companies to integrate and assess cybersecurity risks as part of its overall enterprise risk management. Further, tools, such as National Institute of Standards and Technology's (NIST) Cybersecurity Framework, are designed specifically to enable non-cybersecurity experts to manage cybersecurity risk at the executive level.

Moreover, although the proposal includes a safe harbor from liability for board members that are designated as cybersecurity experts, this requirement may unfairly intensify scrutiny on such board members if a material incident occurs.

We believe that proposed Item 407(j) may cause companies to prioritize cybersecurity expertise on the board of directors to the detriment of other cybersecurity measures and other desired experience.

Proposed Item 407(j) also may negatively impact overall cybersecurity across companies. Cybersecurity standards like the NIST Cybersecurity Framework, Center for Internet Security (CIS) Top 20 Critical Security Controls, International Organization for Standardization (ISO) standards, and Service Organization Controls (SOC) all follow a risk-based approach to cybersecurity. The opportunities to enhance cybersecurity programs and purchase more tools and software are limitless while budgets are not. With this disclosure requirement, companies may feel additional pressure to spend more money and resources on having a board member with cybersecurity expertise, even at the expense of other cybersecurity initiatives that might make the company more secure. This requirement may tip the scales on this particular and specific control in a way that does not actually consider the specific risks to the company and the best ways to remediate those risks. A 2022 industry survey recently reported that only 11% of S&P 500 directors disclosed cybersecurity expertise, which suggests there already is a shortage of cybersecurity expertise among board members.[1] This issue may be exacerbated by more companies competing to find members with cybersecurity expertise on their boards of directors, which may make it even more challenging, and thus more expensive, to bring in and retain such board members.

---

[1] MyLogIQ. (March 2022). *Company IQ Cybersecurity Oversight Benchmarking Report*, available at Files.mylogiq.com/Link_Files/ReportFiles/Cybersecurity%20Oversight%20Benchmarking%20Report%20March%202022%20.pdf.

In addition, as companies attempt to create balanced and effective boards of directors with the appropriate experience needed for their specific situation, the required disclosure may put pressure on companies to prioritize candidates with cybersecurity experience over other desired qualifications, whether based on their industry, regulation or shareholder requests.

We believe that Proposed Item 407(j) should be broader, such as providing disclosure of how the board of directors obtains sufficient cybersecurity expertise and expanding on the list of qualifications for cybersecurity expertise.

While we do not contest that the board of directors should dedicate specific time and energy to cybersecurity risk, specific technical expertise on the board of directors is not required to do so. Similar to how the board of directors of a company with broad international exposure may hire a geopolitical advisor to help it assess geopolitical risks, board members may choose to rely on third party experts to answer technical questions, while equally and competently managing cybersecurity risks. As such, we recommend that the Commission consider having companies disclose how boards of directors obtain sufficient cybersecurity expertise, rather than narrowly require a member of the board to have cybersecurity expertise.

However, if the Commission chooses to require disclosure of cybersecurity expertise of specific board members, the Commission should broaden the non-exclusive list of qualifications. Expertise in areas like incident response, security architecture and engineering, and securities operations do not necessarily translate into skills necessary for enterprise-wide cyber risk management (any more so than being a skilled deposer of witnesses makes one prepared to manage a complex trial or being a carbon offset expert makes one qualified to mitigate climate change effects on a company's business). While these specific skillsets demonstrate hands-on understanding of portions of cybersecurity, they do not translate into the ability to provide guidance and direction to management on how to prioritize, manage, and transfer risk. Instead, requiring board members to have these specific skillsets may result in the appointment of board members who become focused on specific areas in which they have knowledge rather than on the broader risk management.

While serving as a Chief Information Security Officer may be directly on point, skill sets such as risk management in a technology company, serving as a chief compliance or risk officer, or other risk management background are more likely to be relevant than specific technical expertise.

We appreciate the opportunity to provide these comments regarding the Cybersecurity Reporting Proposal. If you have any questions or comments do not hesitate to contact Beth George, Richard Blake, Jose Macias or Allison Spinner.

Very truly yours,

WILSON SONSINI GOODRICH & ROSATI
Professional Corporation

[redacted]