May 9, 2022

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

RE: File Number S7-09-22

Dear Ms. Countryman:

We appreciate the opportunity to comment on the Securities and Exchange Commission (the SEC or the "Commission") proposed rule, *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*. We are pleased to provide our perspectives on this important topic, which CEOs cited as the greatest threat to their companies in PwC's Global CEO Survey released in January 2022.

Overall, we support enhanced disclosure related to cybersecurity risk and the Commission's efforts to standardize cybersecurity disclosures for all public companies. We recognize the importance of a registrant's obligation to provide its investors with timely, accurate, and decision-useful information on cybersecurity.

Although we are supportive of the proposed rules, we offer recommendations in the appendix that we believe will clarify the requirements and make the rules more operational for registrants while still meeting the needs of investors. Our intent in providing these recommendations is to balance the need to provide timely, decision-useful information to investors, while also mitigating a registrant's exposure to risk from bad actors.

* * * * *

The appendix includes our detailed recommendations, organized by section. We would be pleased to discuss our comments or answer any specific questions that the Commission or its staff may have. Please contact Mary Grace Davenport at mary.grace.davenport@pwc.com or Heather Horn at heather.horn@pwc.com regarding our submission.

Sincerely,

PricewaterhouseCoopers LLP

PricewaterhouseCoopers LLP

PricewaterhouseCoopers LLP, 400 Campus Drive, Florham Park, NJ 07932
T: (973) 236 4000, F: (973) 236 5000, www.pwc.com

Appendix

Section B: Reporting of Cybersecurity Incidents on Form 8-K

We agree with the proposed requirement to disclose material cybersecurity incidents. Limiting disclosures to information that is material per the securities laws helps disclosure remain relevant for investors. Under the SEC's Division of Corporation Finance's current interpretive guidance, registrants already assess the materiality of cybersecurity incidents for disclosure and should have effective policies and procedures established to do so. We note that completing a materiality determination could take several weeks to months from initial identification of an incident, depending on its complexity. Thus, we support the requirement to determine that an incident is material as soon as reasonably practicable. In addition, we agree with the proposed limited safe harbor with regard to the consequences of an untimely Form 8-K filing under proposed Item 1.05.

The proposed rule would require disclosure of material cybersecurity incidents even if a government, a government agency, or law enforcement has instructed the registrant not to disclose the information for a period of time. We believe governmental prohibitions on disclosure should take precedence. As such, we recommend that the Commission modify the proposed rule to require disclosure on Form 8-K the later of four business days after determining the incident is material and the date disclosure is no longer restricted by a government or agency.

Given the proposed time frame for disclosure, some information may be incomplete or unavailable. In particular, it may be harder to compile information about third-party resources (which would be included in the disclosure requirements based on the proposed definition of "information system"). We acknowledge that the registrant's responsibility for the cybersecurity of its operations extends to systems it uses but does not own. However, because of the possible difficulty in obtaining information from a third party because of an unwillingness to share information before an investigation is finalized or a limitation on contractual rights, the related Form 8-K may be filed with less detail than if the system were owned. We believe, however, that even limited information, filed in a timely manner, will be useful to investors. We also agree with the proposed safe harbor for registrants who may be unable to include all of the required disclosures in the Form 8-K at the time of filing.

Some of the information required to be disclosed, such as whether the incident has been remediated, could subject the registrant to increased cybersecurity risk. When a particular incident is resolved, disclosing that remediation of that incident is complete may suggest that the risk itself is resolved when, in reality, companies are continuously improving their security posture and adjusting to changes in the threat landscape. At the same time, disclosing that remediation is in process or has not yet begun suggests that the company may still be vulnerable to some of the underlying aspects of the attack. Although the proposal indicates that the Commission "would not expect a registrant to publicly disclose specific, technical information about its planned response to the incident or its cybersecurity systems, related networks and devices, or potential system vulnerabilities in such detail as would impede the registrant's response or remediation of the incident," even a lack of disclosure on this point may provide bad actors with too much information, inviting additional breaches. As a result, we recommend removing remediation from the list of required disclosures.

We note that some cybersecurity incidents result in loss of assets, often made possible by unauthorized access to information. However, the proposed requirements do not explicitly address including asset loss in the disclosure. We recommend that the disclosure of the nature and scope of the incident include whether any cash, securities, inventory, or other tangible or intangible assets were lost as a result of the incident.

Section C: Disclosure about Cybersecurity Incidents in Periodic Reports

C1 - Updates to Previously Filed Form 8-K Disclosure

We support the proposal's requirement to provide material updates to cyber incident information included in a Form 8-K in subsequent Forms 10-Q or 10-K. However, the proposed rules are unclear regarding the registrant's obligation to file an amended Form 8-K. Clarity on when the registrant would be obligated to amend the Form 8-K would ensure registrants comply with the disclosure requirements and help management consider the implications of possessing material nonpublic information as it pertains to insider trading protocols.

We also observe that proposed Item 106(d)(1) of Regulation S-K would require a registrant to include in its update of prior incident disclosures, as applicable, a description of the *potential* material future impact of the incident on operations and financial condition. This provision is vague, and it is unclear how a registrant would determine if there is a potential material future impact. We recommend removing this example from the list of matters that should be addressed.

C2 - Disclosure of Cybersecurity Incidents that Have Become Material in the Aggregate

The proposing release refers to the need to analyze related cybersecurity incidents and consider them for disclosure when they become material in the aggregate. We agree that there may be times when a series of incidents should be reported together because they are collectively material. We note, however, that proposed rule 229.106(d)(2) refers only to the need to aggregate a "series of previously undisclosed individually immaterial cybersecurity incidents." We recommend that the final rules make it clear that only related incidents need to be considered when assessing whether they are material in the aggregate. We do not support the aggregation of different types of incidents; it would be challenging and perhaps not operationally feasible since:

- materiality assessments may vary by incident type,
- it would be challenging to provide clear and comparable disclosures of aggregate incidents without common underlying characteristics, and
- if the incidents are unrelated, the registrant would be disclosing (and updating) specifics on remediation of individually immaterial items.

As there is no guidance provided in the proposed rule on how to aggregate previously undisclosed related incidents, we recommend that the Commission include principles-based guidance to help ensure consistency in application. The guidance should be sufficiently flexible to accommodate the myriad of cybersecurity incidents that registrants of different sizes and sophistication and across different industries would need to consider, but set an appropriately high bar for when incidents need to be considered in the aggregate. Such aggregation guidance could be similar to that used to aggregate deficiencies in audits of ICFR. For example, when determining whether to aggregate deficiencies related to cybersecurity, management often considers the nature of the incidents and the systems impacted, as well as the interaction of systems and entry points and whether the incidents are addressed by the same remediation. Additional guidance regarding the time period over which incidents should be aggregated would also be helpful for consistent application. Any guidance issued by the SEC should allow for management to exercise well-reasoned judgment regarding which incidents should be aggregated.

Section D: Disclosure of a Registrant's Risk Management, Strategy and Governance Regarding Cybersecurity Risks

D1 - Risk Management and Strategy

We support disclosure of a registrant's risk management policies and strategy pertaining to cybersecurity, and agree that cybersecurity risks may have an impact on a registrant's business strategy, financial outlook, or financial planning. However, we believe these disclosures, like all disclosures, should be rooted in materiality. As proposed, registrants would need to disclose whether cybersecurity-related risk and incidents have affected or are "reasonably likely to affect" the registrant's results of operations or financial condition and if so, how. There does not appear to be an explicit materiality qualification in this proposed requirement. We recommend that the proposed rule refer instead to cyber incidents that are "reasonably likely to have a material impact" on the results of operations or financial condition.

We agree with the proposed disclosure of whether the registrant has policies and procedures to oversee and identify the cybersecurity risks associated with its use of any third-party service provider. We note that one way for companies to assess and monitor third-party providers is by obtaining reports from licensed CPA firms who can provide assurance about the third party's cybersecurity controls and disclosures.[1]

D2 - Governance

Under the proposed rules, registrants would be required to disclose information about their board's oversight of cybersecurity risk. We agree that understanding how the board oversees this risk in particular is important. We believe, however, that there is value in co-locating all governance-related disclosures. Item 407(h) of Regulation S-K requires a description of the extent of the board's role in the risk oversight of the registrant, such as how the board administers its oversight function. We would support amendments to Item 407 to require that the detail of the board's oversight include a discussion of how it oversees cybersecurity risk.

D3 - Definitions

We recommend that the Commission align its definition of a cybersecurity incident with the definition used by the National Institute of Standards and Technology (NIST), which defines a cybersecurity incident as "a cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery." NIST separately defines a "cybersecurity event" as "a cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation)." We believe utilizing an existing, widely used, and commonly understood definition is preferable to creating an alternate SEC-specific definition.

If the Commission elects to retain a separate definition, we recommend that the definition be modified to make clear that a cybersecurity incident requiring disclosure should be an actual breach (i.e., a system was actually exploited versus jeopardized).

Section G: Structured Data Requirements

We support the proposal to require block text and detailed tagging of the narrative and quantitative disclosures required by the proposal using Inline XBRL. The provision of structured data will make this information more easily accessible for purposes of aggregation, comparison, and other filtering by investors and other market participants.

[1] The AICPA's cybersecurity reporting framework may provide suitable criteria to be used in evaluating cybersecurity at service providers.