Tel: 312-856-9100
Fax: 312-856-1379
www.bdo.com

330 North Wabash, Suite 3200
Chicago, IL 60611

May 9, 2022

Office of the Secretary
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, D.C. 20549-1090

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

Dear Office of the Secretary:

This letter is the response of BDO USA, LLP to the proposed rule amendments referred to above.

We support the Commission's efforts to improve the timeliness and nature of disclosures made about material cybersecurity incidents and registrants' undertakings to manage and mitigate material cybersecurity risks. The prevalence of significant cybersecurity incidents, as well as the increasing and often substantial costs associated with such incidents highlight the need for companies to communicate timely and accurate information related to these events to their investors. We believe investors are best suited to provide feedback about the utility of the proposed disclosures and that registrants are best suited to provide feedback about the operational feasibility of providing the proposed disclosures in the specified timeframes. However, we have several observations about the clarity and application of the rules that the Commission may wish to consider when drafting the final amendments.

Proposed Disclosures in Form 10-K

We generally support the proposed approach to include the required cybersecurity disclosures in a separately captioned section of Form 10-K. However, we note that proposed Item 1.C., would require registrants to furnish all information required by proposed Item 106 of Regulation S-K, which includes cyber risk management and strategy (106(b)), governance (Item 106(c)), and updated incident disclosure (Item 106(d)). We believe the requirement to disclose the board's oversight of cybersecurity risks under Item 106(c)(1) would be better placed within Part III, Item 10 of Form 10-K where the registrant makes its other disclosures about corporate governance matters. Registrants often incorporate Part III information of Form 10-K by reference from their proxy statements that are filed at a later date. We wondered whether the Commission intended cybersecurity governance disclosures to precede disclosure of all governance matters related to a registrant. Accordingly, we recommend moving the proposed Item 106(c)(1) disclosure requirements into Item 407, *Corporate Governance*, of Regulation S-K to better align the disclosures with the framework for disclosure on other governance matters.

Separately, we note proposed Item 106(d) of Regulation S-K would require companies to disclose when a series of previously undisclosed and individually immaterial cybersecurity incidents have become material in the aggregate. However, the timeframe over which these incidents need to be evaluated to trigger such a disclosure is not clear. Should registrants evaluate the requirement based on the period presented in the periodic report (e.g., the latest fiscal year or interim period)? Do they need to consider aggregation over all periods included in the periodic report? Absent clarifying guidance, some may interpret the timeframe to be open-ended (such that registrants would need to track and perpetually aggregate the impact of incidents that span fiscal periods, an outcome which we believe is unlikely to produce meaningful disclosure about material cyber incidents). We also have questions about how to interpret the intended breadth of the disclosure requirement. While the proposing release acknowledges that incidents can take a variety of forms, the example is that of "one malicious actor" who engages in numerous small but continuous cyber-attacks "related in time and form against the same company," which may need to be disclosed if the incidents were material in the aggregate. Is the intent of the requirement to address these repeated attempts and attacks from the same party or multiple parties? How should registrants think about whether the incidents represent a "series" of previously undisclosed incidents? If the incidents relate to different systems at different times by different malicious actors (or any variation thereof that is not continuous attack by one malicious actor on the same system), are those to be flagged for potential aggregation? Registrants may face significant challenges making such a requirement operational. In light of these questions and to promote clarity for preparers, we encourage the SEC to address the timeframe and breadth of this disclosure requirement.

Board Cybersecurity Expertise

Proposed Item 407(j) of Regulation S-K would require a registrant to disclose if any member of the board of directors has expertise in cybersecurity, including the names of such directors and any details necessary to describe the nature of their expertise. While we recognize the importance of cybersecurity expertise at the board level, we note that boards fulfill the need for 'expertise' in different ways depending on registrant-specific facts and circumstances. For some companies, a board member with requisite cybersecurity expertise may be warranted. For others, while board members understand the registrant's material cybersecurity risks, policies, and incidents, they may supplement their knowledge needs with the use of outside advisors and experts in lieu of having board member 'expertise.' We support the ability of companies, their boards, and shareholders to consider what level of expertise is most beneficial to the organization and how that need will be satisfied (whether internal or supplemental external support for the wide array of topics a board must address). We wonder whether the requirement to explicitly disclose board-level cybersecurity expertise may cause companies to seek out members with cybersecurity expertise, even if the board or registrant would benefit more from expertise in other areas. We suspect this will be a challenging exercise, particularly for smaller companies when the pool of board candidates with this type of expertise may be limited. Smaller boards (e.g., of five individuals) may face similar challenges. Consequently, we believe the SEC should consider whether the existing disclosure requirements of

Item 401 of Regulation S-K[1] about board expertise are sufficient without placing undue emphasis on cybersecurity above other material risks and business needs.

Phased Compliance

The proposing release notes that the cost of the proposed amendments for smaller companies might be disproportionately high compared to larger companies but the costs of an attack could be more detrimental. While the benefits of the proposed disclosures may outweigh the costs associated with making them, the Commission may consider a longer transition period for smaller reporting companies. We believe that there may be an opportunity to mitigate some of the disproportionate cost by allowing them to benefit from any implementation lessons and disclosures made by larger companies. This transition period would also allow these companies more time to organically develop or outwardly obtain the necessary expertise to comply with the proposed requirements.

* * * * * * * * * * * * *

We appreciate this opportunity to express our views to the Commission. We would be pleased to answer any questions the Commission or its staff might have about our comments. Please contact Tim Kviz, National Assurance Managing Partner – SEC Services, at [redacted] or via e-mail at [redacted], or Phillip Austin, National Managing Partner – Professional Practice and Audit, at [redacted] or via e-mail at [redacted].

Very truly yours,

BDO USA, LLP

[1] Item 401 of Regulation S-K requires registrants to discuss the specific experience, qualification, attributes or skills that led to the conclusion that a person should serve as a director for the registrant. This disclosure also contains information about the person's particular areas of expertise or other relevant qualifications. We believe the disclosures in proposed Item 106(c)(1) may not be necessary.