Deloitte & Touche LLP
695 East Main Street
Stamford, CT 06901-2141

Tel: [redacted]
Fax: [redacted]
www.deloitte.com

May 9, 2022

Ms. Vanessa A. Countryman
Secretary
U.S. Securities and Exchange Commission
100 F Street N.E.
Washington, DC 20549

Re: **File Reference No. S7-09-22;** *Request for Public Input on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure* (SEC Release No. 33-11038; the "proposed rule")

Dear Ms. Countryman:

Deloitte & Touche LLP is pleased to respond to the Commission's March 9, 2022, request for public input on cybersecurity risk management, strategy, governance, and incident disclosure. We appreciate the opportunity to provide observations from our role in the capital markets (e.g., current practices, company readiness, and key drivers of decision-useful disclosure) that may be helpful to the Commission as it considers the next steps for the proposed rule, as well as to suggest certain areas where we believe that clarification could assist issuers in providing consistent and comparable information to investors.

Observations from Our Participation in the Capital Markets

While executives, boards, and audit committee members generally acknowledge the increasing importance of cybersecurity matters, in our work with companies within the capital markets, we have observed a wide variation in where companies are on the journey to integrate cybersecurity considerations into their enterprise risk management system, strategy, and core business activities. We have also seen significant variation in what each company measures and reports. Many issuers have a robust infrastructure to identify, define, measure, and communicate cybersecurity matters while certain other issuers may still be developing and implementing cybersecurity infrastructure into core business functions.

As the Commission moves forward in addressing cybersecurity matters in its disclosure regime, it will be important to consider these variations among companies, and how they may affect the ability to elicit useful, reliable, and comparable cybersecurity disclosure across all SEC reporting companies.

Our observations about the variation in company practice on cybersecurity reporting matters include the following:

1. Issuers face challenges in assessing cybersecurity incidents at third-party service providers (TPSPs).

   Issuers will have to rely on TPSPs to provide timely and complete information on cybersecurity incidents to meet their disclosure requirements under the proposed rule. This will require that the TPSPs also have a robust infrastructure to identify, define, measure, and communicate cybersecurity matters. The responsibility for identifying, notifying, and remediating cybersecurity matters at the third party may rest with the TPSP if this is specified in the contractual arrangement with that TPSP. However, there is a risk, not completely within an issuer's control, that the TPSP (1) may not notify an issuer of an incident, (2) may not communicate timely, or (3) may not provide sufficient details on the incident to allow the issuer to evaluate the risk and/or materiality of the incident or the related remediation process. Further, many TPSPs involve other subservice organizations in the delivery of their services. This adds another layer between the issuer and the service organization in terms of obtaining information on an incident.

   Certain TPSPs and subservice organizations may be receiving Service Organization Controls (SOC) reports, which include an independent attestation covering the controls over issuers' data at such TPSPs. However, not all companies receive such reports, and there are limitations regarding their use. For example:

   - SOC 1 reports focus on internal controls over financial reporting and therefore would not provide a complete picture of controls over relevant information given the breadth of the cybersecurity disclosures.
   - SOC 2 reports focus on operational objectives and have specific requirements that cover the Trust Services Criteria[1] (including up to five categories of security, availability, processing integrity, confidentiality, and/or privacy) and therefore may need to be enhanced to include controls over these specific disclosures.
   - Both SOC 1 and SOC 2 reports are typically issued annually, which may not be timely enough for issuers.
   - It may also be difficult for an issuer to use the information in a SOC report to evaluate immaterial incidents in the aggregate because SOC reports are presented from the TPSP's perspective and are the same whether issued to a multi-billion-dollar large accelerated filer or smaller reporting company.

   Given the challenges inherently involved in obtaining timely and decision-useful information from TPSPs, we would suggest that the Commission consider whether providing issuers additional transition time to comply with the requirements to disclose incidents at TPSPs would allow issuers to enhance the reporting infrastructure with TPSPs through updated contractual provisions or other appropriate means.

[1] See the American Institute of Certified Public Accountants' *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy,* available at https://us.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf

2. Issuers may not currently have cyber incident tracking systems designed to support the aggregation of all immaterial incidents.

   As noted above, we have observed varying degrees of sophistication of cybersecurity programs and protocols. While many issuers have a robust infrastructure to identify and communicate cybersecurity matters, certain, less mature issuers may still be developing and incorporating cybersecurity infrastructure into core business functions. Even issuers with mature systems may not have currently designed them to retain details about immaterial cyber incidents. If the final rule retains the requirement to aggregate immaterial cyber incidents and report them when they become material in the aggregate, issuers may need additional time to implement system functionality to support this requirement. Further, issuers may also require further guidance on how to perform this aggregation (e.g., the period over which the information related to immaterial incidents must be retained and assessed). Refer to our observations in *Additional Clarity to Drive Consistent, Comparable, and Reliable Disclosure* below.

3. Cybersecurity has been an area of increasing focus for boards and there are a variety of ways boards exercise their oversight of this area.

   We have observed that oversight of cybersecurity is an increasing area of focus for boards and agree with the Commission that such oversight is a critical aspect of governance. For example, a January 2022 survey of 246 audit committee members conducted by Deloitte and the Center for Audit Quality showed that of those overseeing cybersecurity, two-thirds expected to spend more time on the topic in the coming year.[2] We have also observed that there are a variety of board oversight structures, the most effective of which are tailored to the needs of the company (e.g., taking into account industry, company structure, company maturity). For example, in the Deloitte/CAQ audit committee survey, approximately half of the respondents reported that the audit committee is responsible for overseeing cybersecurity. In other companies, we have observed that board oversight of cybersecurity may rest with the full board or with another committee (e.g., a risk or technology committee).

   We agree with the Commission that board understanding of critical oversight topics is important, including making sure that the CEO hires an experienced C-suite that understands the board's role and how to inform and discuss strategic topics with the board. A board must be informed and knowledgeable enough to advise and challenge management in all areas of its oversight. Boards themselves acknowledged this need,[3] and many use a matrix to define and identify the skills, experiences, and diversity needed to execute their duties effectively. We have observed that upon identifying needed skills, boards can gain such skills in numerous ways, including by recruiting members with specific experience or by educating existing board members individually or collectively.

   We note that in addition to proposing required disclosure about whether any member of a company's board has cybersecurity expertise, the Commission recently proposed similar

---

[2] See Deloitte's and the Center for Audit Quality's jointly published *Common Threads Across Audit Committees:* https://www2.deloitte.com/us/en/pages/center-for-board-effectiveness/articles/audit-committee-practices-report.html?id=us:2em:3na:acb:awa:boardef:020222:mkid-K0148184&ctr=frcta2&sfid=0033000000QOgmZAAT.

[3] In the Deloitte/CAQ survey, 41 percent of respondents indicated that the audit committee needed more cyber expertise (more than in any other risk area).

disclosure related to board expertise in climate-related risks.[4] We believe dedicated expertise may be valuable for some companies. In general, however, especially given the limited size of boards,[5] it may not be practical or advisable for a board to recruit dedicated experts in each of its critical oversight areas. While we recognize that neither of the proposals *requires* designated board experts, we believe that, especially when read together, some may infer that the Commission prefers that issuers identify such experts. We therefore encourage the Commission to consider whether existing proxy rules (which require disclosure of the particular experience, qualifications, attributes, or skills of board nominees), when combined with disclosure regarding board oversight of a company's cybersecurity risk, may be sufficient to inform investors about the role of the board in cyber risk management, without a separate requirement to identify cybersecurity experts.

Additional Clarity to Drive Consistent, Comparable, and Reliable Disclosure

The quality, transparency, relevance, and comparability of cybersecurity disclosures can be enhanced by the application of established standards and frameworks. We have identified several elements of the proposed rule that may benefit from additional clarity and thus help the Commission achieve its goal of eliciting consistent, comparable, and reliable disclosure.

Terminology Definitions

We propose that the Commission consider clarifying certain terminology within the proposed rule, including "any information" in the definition of cyber incidents and "any potential occurrence" in the definition of cybersecurity threats. As written, the term "any" implies considering each and every instance in which either an incident or threat may exist. This broad definition may be applied inconsistently among issuers. While issuers may need to establish a framework to exercise judgment in evaluating incidents, further guidance regarding whether a de minimis concept could apply may assist issuers in focusing on cybersecurity incidents or threats that are more relevant to the organization's purpose and strategy, thereby providing more decision-useful information to investors. The Commission may consider whether there should be tiers of important information and describe the impact on the issuer's evaluation for each tier level. For example, the issuer could apply a risk assessment approach that distinguishes between "crown jewel" information such as strategic intellectual property and personally identifiable information (PII) from lower risk information such as informational data or non-PII internal records that can easily be reproduced. Clarifying the types of information that would be evaluated within the definition of a threat or incident may assist an issuer in focusing disclosure on the information most useful for investors.

We have also considered the intersection of this release and the release *Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies* ("Release No. 33-11028") and would like to highlight that there are certain additional terms defined in Release No. 33-11028 that were not defined in the proposed rule. Thus, we would suggest that the Commission consider whether the defined terms should be consistent. For example, Release No. 33-

[4] See *The Enhancement and Standardization of Climate-Related Disclosures for Investors* (SEC Release No. 34-94478; File No. S7-10-22, available at: https://www.sec.gov/rules/proposed/2022/33-11042.pdf).

[5] According to the 2021 U.S. Spencer Stuart Board Index (available at https://www.spencerstuart.com/-/media/2021/october/ssbi2021/us-spencer-stuart-board-index-2021.pdf) S&P 500 boards range in size from 5 to 22 members, and average 10.8 directors; 71 percent of boards fall into in the 9-to-12-member range.

11028 includes definitions of "adviser information," "cybersecurity risk," and "cybersecurity vulnerability," but these terms or their equivalents are not defined in this proposed rule.

Appropriate SEC Form for Disclosure

It is not unusual for the investigation into a material incident to take months and for facts to develop or become known over the period of investigation. Footnote 69 of the proposed rule states:

> Notwithstanding proposed Item 106(d)(1), there may be situations where a registrant would need to file an amended Form 8-K to correct disclosure from the initial Item 1.05 Form 8-K, such as where that disclosure becomes inaccurate or materially misleading as a result of subsequent developments regarding the incident. For example, if the impact of the incident is determined after the initial Item 1.05 Form 8-K filing to be significantly more severe than previously disclosed, an amended Form 8-K may be required.

We suggest the Commission consider clarifying when material changes, additions, or updates in a cybersecurity incident should be updated via Form 8-K as opposed to a periodic filing. This could include clarifying whether a Form 8-K amendment, rather than an update in a periodic filing, would be required when a material increase in scope and/or severity is uncovered as an investigation into an incident progresses. For example, assume a cybersecurity incident is identified as materially impacting an issuer's systems in one country and that incident was disclosed in Form 8-K. Subsequently, the issuer determines that multiple countries are materially impacted. Is an issuer required to report such development in Form 8-K to "correct disclosure . . . that becomes inaccurate or materially misleading as a result of subsequent developments" or is such a development considered an update to the previously disclosed information?

Framework for Aggregating Immaterial Cybersecurity Incidents

We suggest the Commission consider establishing a framework for aggregating a series of previously undisclosed individually immaterial cybersecurity incidents to determine when they may become material in the aggregate. A framework for aggregation may assist in ensuring comparability and consistency across issuers and enhance the usefulness of such information for investors. More specifically, the Commission may consider addressing the following questions within an aggregation framework:

- Would aggregation restart each annual period or begin on some other date such as inception of the company, from an initial registration statement, or some other defined period? Further, would there be a cutoff date or period specified?
- Should immaterial incidents be categorized by some defining characteristic when assessing aggregation (e.g., type of incident, system impacted, method of attack)?
- Should remediated, immaterial incidents be removed from the aggregation analysis? If so, when?
- How long should such disclosure be maintained in a periodic report once it has been included?
- How would subsequent immaterial incidents be evaluated once disclosure of such incidents in the aggregate is presented?

In evaluating these points, the SEC may consider the application of other SEC rules that provide a framework for disclosure requirements when events aggregate to a defined level, such as that in Regulation S-X Article 3-05, *Financial Statements of Businesses Acquired or to Be Acquired*, which requires assessment of individually insignificant acquisitions for an issuer's fiscal year typically up to the

point of its next 10-K filing. Further, the SEC may also consider providing examples of how the framework is applied, if aggregating immaterial incidents with different defining characteristics is required (i.e., a phishing incident and malware attack) so that issuers may apply the framework consistently, using common parameters.

Transition Provisions and Scalability

As highlighted above, the level and sophistication of cybersecurity reporting structures varies by issuer, and, if the proposed rule were finalized as written, many issuers may need to invest further in their cyber tracking and disclosure systems to meet certain new disclosure requirements. We have observed that larger issuers may currently have systems in place to track some of this information for disclosure more readily, while smaller issuers may require significant investment to implement systems that perform the detailed tracking and evaluation necessary for some disclosures, such as aggregation. Further, issuers that are more prepared to identify and investigate incidents may disclose incidents earlier than those that are less prepared, which may skew information available to investors and cause them to potentially view as more favorable an issuer that has not disclosed a cyber incident because it lacks the resources to identify it. Therefore, we suggest the Commission consider outreach to issuers on the need for extended transition provisions or a phased implementation process by registrant tier to give issuers more time to prepare to provide certain disclosures and, ultimately, produce more consistent, decision-useful disclosures.

* * * *

Given the widespread impact that cybersecurity incidents can have, it becomes increasingly important for investors to seek disclosure about such matters to understand how companies are prepared for such disruptions. We commend the Commission for its timely focus on this area.

We appreciate the opportunity to provide our perspectives on the proposed rule. If you have any questions or would like to discuss our views further, please contact Christine Davine at [redacted] or Sandy Herrygers at [redacted].

Sincerely,

Deloitte & Touche LLP

Deloitte & Touche LLP

cc: Gary Gensler, Chair
Caroline A. Crenshaw, Commissioner
Allison Herren Lee, Commissioner
Hester M. Peirce, Commissioner
Renee Jones, Director, Division of Corporation Finance
Paul Munter, Acting Chief Accountant