May 9, 2022

U.S. Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549

Re: File Number S7-09-22: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure; Release Nos. 33-11038; 34-94382; IC-34529

Dear Office of the Secretary:

The Center for Audit Quality (CAQ) is a nonpartisan public policy organization serving as the voice of U.S. public company auditors and matters related to the audits of public companies. The CAQ promotes high-quality performance by U.S. public company auditors; convenes capital market stakeholders to advance the discussion of critical issues affecting audit quality, U.S. public company reporting, and investor trust in the capital markets; and using independent research and analyses, champions policies and standards that bolster and support the effectiveness and responsiveness of U.S. public company auditors and audits to dynamic market conditions. Based in Washington, DC, the CAQ is affiliated with the American Institute of CPAs. This letter represents the observations of the CAQ based upon feedback and discussions with certain of our member firms, but not necessarily the views of any specific firm, individual, or CAQ Governing Board member.

The CAQ appreciates the opportunity provided by the Securities and Exchange Commission (SEC or the Commission) to comment on its proposed rules to enhance and standardize Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (the proposed rule or release).

CAQ Background and Introduction

The CAQ's members are accounting firms that perform financial statement audits of public companies. Many of these firms provide a wide range of audit and consulting services across all industry sectors, providing them with the opportunity to obtain a practical understanding of the cybersecurity landscape, including risk management, strategy, and governance practices and incident disclosures across a myriad of entities and contexts. Accordingly, our observations in this letter are drawn from many stakeholder groups and various industry sectors. Indeed, the auditing profession is in a strong position

to play an important role in fostering instructive conversations about cybersecurity risk management, bringing to bear its core values—including independence, objectivity, and skepticism—as well as its deep expertise in providing independent evaluations in a variety of contexts.

Public company auditors have been actively engaged in information security for decades, and already provide valued cybersecurity risk management support to their advisory clients. Beginning in 1974, auditors were required to consider the effects of information technology on financial statements. This evolved into the development of attestation engagements dealing with controls at a service organization, as well as other permissible information security consulting services offered to the market.

We are supportive of the transparency that will result through enhancing disclosure by registrants around cybersecurity risk management, strategy, governance, and incident disclosure. As domestic and foreign cybersecurity threats evolve, particularly in the remote and hybrid work environments, timely cybersecurity disclosures are becoming increasingly more relevant and useful to investors and other stakeholders in the financial reporting ecosystem.

We provide below details regarding our overall support for the SEC's efforts to enhance and standardize cybersecurity disclosures for the benefit of both investors and preparers. Clear, operational guidance for registrants will help to ensure that the increased transparency this rule intends to create results in consistent and comparable disclosures.

From the broad perspective we have gained through direct contact with our member firms and our own stakeholder engagement (e.g., chief information officers, internal auditors, audit committee members, academics, and financial reporting executives), we have summarized a number of key observations with respect to the proposed rule. These are organized by thematic area below.

Support of enhanced disclosures

We support the SEC's desire to implement rules that promote consistent, comparable, and decision-useful cybersecurity disclosures and the transparency that comes along with it. Over the years, companies have implemented more technology to support their operations which has created opportunities for unauthorized parties to successfully access, manipulate, and steal sensitive data, misappropriate assets, or disrupt operations. Thus, we agree that stakeholders should be sufficiently aware of companies' cybersecurity risks, policies, strategy, and governance, and provided with timely material breach reporting information in order to make informed decisions regarding those companies.

Increasingly, investors and other stakeholders in the capital markets are beginning to incorporate cybersecurity considerations into their evaluations of registrants. For example, in February 2021, Institutional Shareholder Services Inc. (ISS) announced methodology changes to its Governance QualityScore rating solution, including the addition of 11 new factors concerning information security

risk oversight and management.[1] Similarly, Moody's Investor Service has begun to incorporate cyber risks in firms' credit ratings. According to Moody's Managing Director Derek Vadala, "[w]e view cyber risk as event risk that can have a material impact on sectors and individual issuers."[2] Consistent, comparable information regarding material cybersecurity information is important to inform these stakeholders who interact with the capital markets.

Enhanced cybersecurity disclosures could benefit registrants as well. An academic study also shows that increased disclosure of cybersecurity investments by registrants may decrease their costs of capital. Specifically, it found that, "[a] one standard deviation increase in disclosing cybersecurity investments in SEC filings reduces the cost of capital by 7%."[3] By disclosing such investments and reducing information asymmetry, registrants may be able to access capital more easily as the perceived risk of investing in these companies decreases with disclosure of improvements to cybersecurity hygiene.

Recommendations for clarity of proposed rule and disclosures

Investments in cybersecurity and efforts to disclose related information come at a cost to registrants, especially if the SEC's requirements are not sufficiently clear and operational. Registrants must be able to apply the proposed rule in a manner that provides consistent and comparable information. While the proposed rule, in part, appears to focus on reducing information asymmetry, the Commission should continue to consider how the proposed rule will also influence the behaviors of preparers, investors, and others in the capital markets. Such behaviors, specifically of preparers, ultimately drive disclosure practices required by the proposed rule. The proposed rule should avoid unintended outcomes which may include:

- Unnecessary influence over the composition of board of directors;
- Incomparable or inconsistent disclosure resulting from the misapplication of the proposed rule by preparers due to lack of clarity in definitions;
- Incomparable aggregation of immaterial undisclosed incidents; and,
- Unclear expectations related to the timeframe in making incident materiality determinations.

In considering historical views of cybersecurity regulations, not all market participants are confident that increased regulation improves cybersecurity practices at registrants. Ernst & Young's (EY) 2021 EY Global Information Security Survey found that in 2021 only 35% of CISO respondents thought that compliance with then-existing cybersecurity guidelines drove the right behaviors within their business, down from 46% in the previous year.[4] It also noted that less than one in five respondents describe cybersecurity regulation as an effective way for them to make the case to their boards for additional budget, down from 29% in 2020. While these responses did not contemplate the effects of the proposed rule, it is

[1] See *Cybersecurity risk disclosures and oversight*, EY
[2] See *Disclosure of Cybersecurity Investments and the Cost of Capital*, Havakhor et al
[3] *Id.*
[4] See *2021 EY Global Information Security Survey*, EY

important that the proposed rule fosters the desired disclosure outcomes by enhancing conduct at the enterprise level. This requires clear and operational rules.

We have also included an appendix to this letter which 1) provides clarification regarding the involvement of the auditor in the disclosure of Other Information including cybersecurity disclosures in Other Information and 2) highlights certain aspects of what assurance over cybersecurity information looks like today and could look like in the future. It also contains educational information regarding a cybersecurity disclosure framework developed by the AICPA which may be useful to registrants.

Qualified talent – organizational and board of directors

While some companies may have in place reasonable cybersecurity risk management policies, governance structures, and strategies, the disclosure requirements in the proposed rule may require significant investments in personnel. We agree that it is important that registrants have appropriate oversight of their cyber risk management, and its disclosure is relevant to investors. It is also important to recognize that registrants have varying needs in these regards, particularly as it relates to oversight. The board of directors needs to be informed about cybersecurity which can be achieved through certain proposed items in the rule; and while a committee may be responsible for oversight of cybersecurity risk management, the requirement to disclose board member expertise as it relates to cybersecurity may be redundant to other proposed disclosure requirements.

Proposed Item 106(c)(1) would require the disclosure of the processes by which the board is informed about cybersecurity risks, and the frequency of its discussions on this topic. We believe this disclosure provides investors with sufficient insight into how boards obtain information regarding cybersecurity risks to inform their oversight. This could include board expertise, if necessary, based on the cybersecurity risk profile of a registrant; however, it provides registrants the flexibility for their boards to obtain cybersecurity information in ways that best suit the organizations they oversee.

As written, the proposed rule focuses on disclosing cybersecurity expertise at high levels within an organization. Expertise is a higher bar than having sufficient knowledge and understanding of a subject matter. In many cases, boards of directors having sufficient knowledge and understanding of cybersecurity risks (and any other relevant risks) facing the registrants they oversee, rather than specific expertise in one area of focus, gives them the ability to execute appropriate oversight activities. Depending on the cybersecurity risk profile of an organization, a board may be able to obtain relevant cybersecurity knowledge and affirm understanding by having expert individuals within an organization through periodic training, knowledge-sharing, and other activities.

While board-level cybersecurity expertise may be appropriate for certain registrants, for others the board can execute reasonable cybersecurity risk management oversight without having such a specific expertise. It should be at the discretion of registrants to determine the level of board cybersecurity expertise required and the manner which boards obtain such expertise. As boards of directors are generally limited in capacity, requiring disclosure of board cyber expertise may result in boards shifting

their composition to prioritize cyber expertise over other important areas of focus to the detriment of overall corporate governance.

Registrants appear to be naturally moderating levels of board cybersecurity expertise to meet their needs. According to a report by EY, "[i]n 2021, 65% of boards [at Fortune 100 companies] disclosed cybersecurity as an area of expertise sought on the board or cited in a director biography, up from 36% in 2018. Notably, a majority (56%) now cite cybersecurity in at least one director biography, up from 44% last year and 27% in 2018"[5]. With demand for cybersecurity expertise already on the rise due to natural demand, the implementation of this aspect of the proposed rule may unnecessarily intensify this issue by increasing the demand for such expertise when it is not needed for all registrants. Therefore, we do not believe it is necessary that registrants disclose board expertise regarding cybersecurity.

Definitions

Proposed definitions – Section II.D.3 of the proposed rule defines the terms "cybersecurity incident" and "cybersecurity threat" (among others) used in proposed Item 106 and proposed Form 8-K Item 1.05. It is important that these definitions are clear and consistent with the definitions and practical applications of such terms in existing or proposed rules, standards, guidance, or other materials put out by the SEC and other standard setting or authoritative bodies.

We do not find that these definitions are sufficiently clear such that all registrants will be able to apply them in a consistent manner. This could have an adverse effect on assessments of materiality, incident disclosures, and other periodic disclosures prepared by registrants. It would be useful for the SEC to clarify these definitions and how they should be applied with practical examples such that they can be operationalized by registrants as intended.

For example, both the definitions of "cybersecurity incident" and "cybersecurity threat" refer to the scope of information to be considered for either an incident or a threat to be "any information [within an information system]."[6] This is a very broad term and could be interpreted differently by registrants, detracting from consistent application and disclosure. The definitions would be clearer if instead it qualified such information using common, risk-based terminology like "confidential", "non-public", or "personally identifiable." The AICPA also defines the term "sensitive information"[7] which encompasses these concepts and others which may be of relevance. Qualifying the types of information for consideration within a cybersecurity threat or incident will provide registrants with a clearer

[5] See *Cybersecurity risk disclosures and oversight*, EY

[6] See Section II.D.3 within the proposed rule

[7] "Sensitive information varies from organization to organization but often includes nonpublic information such as the following: regulatory compliance information; financial information used for both internal and external reporting purposes; confidential sales information, including customer lists; confidential wholesale pricing information and order information; confidential product information including product specifications, new design ideas, and branding strategies; and proprietary information provided by business partners, including manufacturing data, sales and pricing information, and licensed designs. Sensitive information also includes personal information." *Information for service organization management*, AICPA

understanding of these definitions and focus them on areas of importance and decision-usefulness to investors.

We also looked to the definitions of these terms included in the SEC's proposed rule on Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies (the Proposed SEC Investment Advisor Cyber Rule) which qualifies that the information to be considered as part of a cybersecurity incident or threat is "any **advisor** information" [emphasis added]. "Advisory information" is then separately defined.[8] This provides a clearer expectation of the information relevant to a cybersecurity incident or threat. The proposed rule should provide similar clarity.

Consider a situation in which it may be unclear as to whether an incident qualifies as a cybersecurity incident under the proposed definition:

> A phishing email designed to appear to be from the CFO of a registrant directs the Controller of that registrant to wire a payment to an account controlled by the phishing perpetrator. The controller wires those funds to the perpetrator's account.

This may meet the criteria of "an unauthorized occurrence on or conducted through a registrant's information systems"; however, this incident may not meet the criteria of "[jeopardizing] the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein." Clarity of these definitions is important to ensure comparable application by registrants.

Cybersecurity – The proposed rule does not define the term "cybersecurity". We recommend that the proposed rule is revised to include a definition for this term in line with the definition established by the National Institute of Standards and Technology's (NIST). This is a well-known definition and would be a useful addition to the rule text.

> NIST "cybersecurity" definition[9]: "Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."

Aggregation and continuous reporting

Proposed Item 106(d)(2) would require disclosure when a series of previously undisclosed individually immaterial cybersecurity incidents become material in the aggregate. A principles-based framework to guide how such aggregation should be performed would lend to consistency and comparability of these disclosures by registrants. This should include examples of when a registrant would or would not aggregate incidents.

[8] See Section 275.206(4)-9(c) of the Proposed SEC Investment Advisor Cyber Rule.
[9] See NIST's definition of cybersecurity at its *Computer Security Resource Center Glossary*

The proposed rule does not specify a lookback period over which aggregation should be performed. Preparers may interpret this as going back to inception, going back to initial registration with the SEC, or some other period. Once an aggregate set of immaterial undisclosed incidents is reported, it is not clear if preparers should consider subsequent immaterial cybersecurity incidents for inclusion with those previously disclosed in aggregate or if a new clock starts for aggregating immaterial cybersecurity incidents.

The proposed rule also states,

> "While such incidents conceptually could take a variety of forms, … they are either quantitatively or qualitatively material, or both."

This could be interpreted to mean that dissimilar, undisclosed immaterial incidents, for example a malware attack by Attacker A and an unrelated ransomware attack by Attacker B, should be aggregated to assess for materiality. We are not clear if this is the intent of the Commission; however, we find that this would be impractical given that 1) materiality assessments may vary by incident type and 2) preparers would be significantly challenged to provide clear and comparable disclosures of aggregate incidents without at least some common underlying characteristics. If this is the intent of the proposed rule, examples of the application of this concept will be important to ensure consistent execution by registrants.

In considering the period for which incidents, material either individually or in the aggregate, are disclosed, the proposed rule does not state for how long a registrant must continuously disclose such incidents through periodic reports. We believe that as time progresses, there is a diminishing benefit to decision usefulness in continuous reporting, particularly if the incident has been remediated. Continued disclosure of such incidents may have unwarranted negative consequences on a registrant, for example stock price, capital raising, and reputational impacts. Absent any material changes, additions, or updates to previously reported incidents, the proposed rule should specify for how long previously reported incidents must be continuously disclosed.

A framework for aggregation and disclosure timeframe should address the period over which aggregation should be considered, how undisclosed immaterial incidents should be aggregated, and the duration for which continued periodic disclosure is required.

Discovery and materiality determination

We support the SEC's desire to ensure timely reporting of cybersecurity incidents so relevant stakeholders can make informed decisions regarding their relationships with a registrant. We also acknowledge that the SEC expects registrants to make materiality determinations promptly to support timely disclosure of material incidents. We believe the SEC should provide examples of materiality determination timelines to clarify its expectations.

The text of the release states, "we expect registrants to be diligent in making a materiality determination in as prompt a manner as feasible. To address any concern that some registrants may delay making such a determination to avoid a disclosure obligation, Instruction 1 to proposed Item 1.05 states a registrant shall make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident."[10] This may suggest that such determinations should be made more quickly than current interpretive guidance indicates. If the intent of this statement is to accelerate or make more consistent the materiality determination timeline across registrants, we encourage the SEC to revise the proposed rule to include examples regarding what reasonable materiality determination timelines may be as noted in Question 8 of the release. We do not expect that these examples would be all-inclusive; however, we believe they would be useful in providing registrants with additional context and factors to consider in making materiality determinations grounded in the facts and circumstances of cybersecurity incidents they may experience. Registrants already evaluate the severity of cybersecurity incidents as they occur; and absent additional guidance, we expect that registrants will continue to use current practices in doing so.

We acknowledge that this language may also be a means to codify current practice. According to a study by Audit Analytics, in 2021, it took, on average, 42.2 days to discover and 79.8 more days to disclose a breach.[11] We acknowledge that the disclosure decision is not predicated on the materiality determination proposed in this rule; however, this data shows that even after discovery it takes registrants time and due diligence to assemble information to provide to stakeholders. The time taken is necessary to determine the extent of an incident, assess what information or information systems have been impacted, and ultimately determine whether it has had a material impact on the financial statements and/or internal controls.

At the date of discovery, very little may be known about an incident and registrants may be significantly challenged to conclude promptly whether an incident is material. While the date of the registrant's materiality determination may coincide with the date of discovery of an incident, as stated in the proposed rule, we expect that would be rare as most incidents are not simple. The determination of materiality should be thorough and thoughtful such that a registrant does not include inappropriate or incomplete disclosures. Examples may supplement the significant judgements registrants make in cyber incident materiality determinations and could prevent premature disclosure. Premature disclosure could have unintended consequences such as destruction of data by a bad actor, impeding an investigation, or adverse reactions by the capital markets resulting from incomplete information. Registrants should be encouraged to gather and vet meaningful details and context to provide informative disclosures to stakeholders, particularly if a breach is particularly complex or ongoing.

Examples of materiality determination and timelines may aid registrants in balancing the need for timeliness and decision-usefulness of cybersecurity incident disclosure.

[10] See page 22 of the release.

[11] *Trends in Cybersecurity Breaches Disclosures*, Audit Analytics

XBRL

The proposed rule would also require Inline XBRL tagging of cybersecurity disclosures. We support this proposal and agree that Inline XBRL tagging would provide more readily available and easily accessible information to investors, market participants, and others for aggregation, comparison, filtering, and other analysis.

****

The CAQ appreciates the opportunity to comment on the proposed rule and would be pleased to discuss our comments or answer any questions that the Staff or the Commission may have regarding the views expressed in this letter. Please address questions to Dennis McGowan [redacted] or Taylor Harris [redacted].

Sincerely,

Dennis J. McGowan
Vice President, Professional Practice
Center for Audit Quality

cc:
SEC
Honorable Gary Gensler, Chair
Caroline A. Crenshaw, Commissioner
Allison Herren Lee, Commissioner
Hester M. Peirce, Commissioner
Paul Munter, Acting Chief Accountant, Office of the Chief Accountant
Diana Stoltzfus, Deputy Chief Accountant, Office of the Chief Accountant
Renee Jones, Director, Division of Corporation Finance
Lindsay McCord, Chief Accountant, Division of Corporation Finance

PCAOB
Erica Y. Williams, Chair
Duane M. DesParte, Board member
Christina Ho, Board member
Kara M. Stein, Board member
Anthony C. Thompson, Board member
Barbara Vanich, Acting Chief Auditor

Appendix – Auditors and Other Information and assurance over cybersecurity disclosures

Auditors and Other Information

Per the proposed rule, registrants will make these new cybersecurity disclosures in current reports or periodic reports outside of the financial statements. Thus, they are not subject to internal control over financial reporting (ICFR). Rather they will be subject to disclosure controls and procedures and perhaps a reason the requirements are more prescriptive. While the proposed rule would substantially increase disclosures related to cybersecurity, the auditor's role in relation to periodic filings by a registrant has not changed. This could increase confusion between what users of financial statements *believe* auditors do and what auditors *actually* do with respect to cybersecurity disclosures included in "Other Information" outside of the financial statements.

To clarify, paragraphs 4 and 5 of the Public Company Accounting Oversight Board (PCAOB) Auditing Standard 2710, *Other Information in Documents Containing Audited Financial Statements*, (AS 2710) describes the auditor's responsibilities for disclosures in documents containing the audited financial statements. AS 2710 requires auditors to read the other information in documents containing the audited financial statements and consider whether such information or the manner of its presentation is materially inconsistent with information appearing in the audited financial statements or contains a material misstatement of fact. This involves substantially less work than that required in an audit. Even if a company has extensive disclosures in MD&A about its cybersecurity risk management program, the auditor is not required to perform any procedures in the audit of the financial statements or ICFR to evaluate the appropriateness of the design and implementation of the company's cybersecurity risk management program or its effectiveness or consider the broader cybersecurity risks that may affect the organization, outside of those that affect the audited financial statements.

Assurance over cybersecurity disclosures

While registrants are not currently required to obtain assurance over their cybersecurity risk management programs or disclosures, some obtain assurance either voluntarily or as a result of other compliance requirements. Analysts and investors consider information about a company's cybersecurity measures to be important when making investment decisions; Boards of directors may want assurance over information to help fulfill their oversight responsibilities related to their companies' cybersecurity programs and the cybersecurity threats; Company management may desire assured information about how business partners (e.g., vendors) with whom they do business manage their cybersecurity risks.

To the extent that there is demand from investors, boards of directors, management, or others, public company auditors can provide assurance over cybersecurity risk management disclosures. Auditors, in their public interest roles, play a significant role in the flow of comparable and reliable information for decision-making. They bring an objective and independent perspective that can enhance the trust and confidence stakeholders have in cybersecurity information that companies report, and utilize frameworks for the consistent performance of such engagements under established attestation

standards. The CAQ's publication, Role of the Auditor in Cybersecurity, provides further details as to the role auditors play in cybersecurity as it relates to the audit of the financial statements and how the auditor's role in cybersecurity could evolve beyond the financial statements to meet the needs of stakeholders.

Auditors can perform an examination engagement in accordance with the American Institute of CPA's (AICPA's) attestation standards. In an examination engagement, a public accounting firm uses a multidisciplinary team—made up of professionals whose core competencies can include credentialed IT and information security specialists—to perform the engagement. Based on the procedures performed and the evidence obtained, auditors provide an independent report on whether management's description of the company's cybersecurity risk management program is presented in accordance with the reporting framework and whether the controls within the program were suitably designed and operating effectively to achieve the company's cybersecurity objectives based on that framework. To enable auditors to conduct the examination, the AICPA developed a reporting framework that provides a common approach to communicating, evaluating, and reporting on company's cybersecurity risk management program. The reporting framework, known as Systems and Organization Controls (SOC) for Cybersecurity (SOC for Cyber), includes three key components designed to assist stakeholders in understanding a company's cybersecurity risk management program: (1) management's description of the company's cybersecurity risk management program in accordance with the AICPA's *Description Criteria for Management's Description of the Entity's Cybersecurity Risk Management Program* (description criteria), (2) management's assertion that the program meets the AICPA's *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (trust services criteria), and (3) the practitioner's opinion. Management can use the description criteria to determine key components of the company's cybersecurity risk management program to communicate in order to meet the information needs of users and the trust services criteria to evaluate the effectiveness of the processes and controls within the program. Auditors can use the same criteria to opine on the cybersecurity risk management program's design and on the effectiveness of controls management has designed and implemented to achieve the organization's cybersecurity objectives. The practitioner's report may assist boards of directors, senior management, and other pertinent stakeholders as they evaluate the effectiveness of their organization's cybersecurity risk management programs.

As noted in the proposed rule, a significant number of cybersecurity incidents pertain to third party service providers and it would require disclosure concerning a registrant's selection and oversight of third-party entities. The AICPA has established a service which may assist registrants to this end: SOC 2, Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy. These reports are intended to meet the needs of a broad range of users that need detailed information and assurance about the controls at a service organization relevant to security, availability, and processing integrity of the systems the service organization uses to process users' data and the confidentiality and privacy of the information processed by these systems.