Approved by the Investor Advisory Committee at the September 21, 2022 Meeting

Recommendation of the Investor as Owner Subcommittee and Disclosure Subcommittee of the SEC Investor Advisory Committee Regarding Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

The Investor Advisory Committee ("IAC") submits the following recommendation in response to the U.S. Securities and Exchange Commission's ("SEC" or "Commission") proposed release, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure ("Proposed Rule" or "Release").[1] The IAC offers its recommendation following a Panel Discussion Regarding Cybersecurity at its March 10, 2022 public meeting.[2]

The Proposed Rule would amend the regulations under the Securities Act of 1933 and Securities Exchange Act of 1934 to require issuers to report information on cybersecurity risk, strategy, and governance, as well as cybersecurity incidents under certain circumstances. Specifically, the Release prescribes the following periodic disclosures from companies:

- Policies and procedures to identify and manage cybersecurity risks;
- Management's role in implementing cybersecurity policies and procedures;
- The Board of Directors' cybersecurity expertise, if any, and information about its oversight of cybersecurity risk; and
- Updates about previously-reported material cybersecurity incidents.

The Proposed Rule also mandates timely reporting of material cybersecurity incidents on Form 8-K. Should the Commission finalize the rule, issuers would be required to present disclosures via Inline eXtensible Business Reporting Language (Inline XBRL).

The IAC supports the Proposed Rule and highlights certain noteworthy aspects below. We also offer our suggestions for the enhancement of the Proposed Rule (and underlying rule changes) before final implementation.

As representatives of the investor community, we are confident investors will benefit from higher-quality cybersecurity risk-related disclosures from issuers that are decision-useful, consistent, and

[1] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 87 Fed. Reg. 16590 (March 23, 2022), https://bit.ly/3RkTBxt. *Also see* U.S. Securities and Exchange Commission, "Fact Sheet: Public Company Cybersecurity; Proposed Rules" (March 9, 2022), https://www.sec.gov/files/33-11038-fact-sheet.pdf.

[2] *See* U.S. Securities and Exchange Commission Investor Advisory Committee Meeting Agenda (March 10, 2022), https://www.sec.gov/spotlight/investor-advisory-committee/iac031022-agenda.htm and Webcast Archive - Part 2 (March 10, 2022), https://www.youtube.com/watch?v=68XeFbIJxCk. The panel was jointly hosted by the Investor as Owner and Disclosure Subcommittees and featured the following panelists: Keith Cassidy, Associate Director for the Office of Technology Controls Program, SEC Division of Exams; Athanasia Karananou, Director of Governance and Research, Principles for Responsible Investment; Joshua Mitts, Associate Professor of Law and Milton Handler Fellow, Columbia Law School; and Jeffrey Tricoli, Managing Director for Technology Risk Management, Charles Schwab.

timely. We believe the proposed amendments are appropriate in this regard, in service of the Commission's core mission to protect investors; support fair competition, efficiency, and capital formation; and serve the public interest by promoting a market environment that is worthy of the public's trust.[3]

Background and Rationale for Reform

The Proposed Rule represents an important next step in the Commission's graduated efforts to ensure investors have access to material information on cybersecurity risks. As noted in the Release, since 2011 the Commission and staff have provided interpretive guidance to issuers regarding cybersecurity risk and incident reporting. These guidance documents, including the 2011 Staff Guidance[4] and 2018 Interpretive Release,[5] sought to improve the quality of cybersecurity-related disclosures to investors through "the application of existing disclosure and other requirements under federal securities laws to cybersecurity risks and incidents."[6] This approach was not unique to the Commission at the time: a 2015 report from the Center for Strategic and International Studies ("CSIS") about financial industry cybersecurity regulation notes that cybersecurity was "rarely" mentioned in existing laws and regulations.[7] The Proposed Rule economic analysis provides examples of rules and regulations where incident reporting may be required, either publicly or to specific governmental bodies and agencies, private organizations, and/or counterparties.[8]

An ever evolving, interconnected, and interdependent technological landscape, along with the increasing sophistication, incidence, and impact of cybersecurity incidents and related risks over the past decade, now necessitate a more comprehensive approach to cybersecurity risk management and mitigation within the securities regulatory framework. The Proposed Rule provides a comprehensive review[9] of these risks and attendant impacts across the U.S. capital markets, from individual issuers to systemic risks threatening the U.S. economy and broader national security infrastructure, which we will not repeat here. These risks, and the costs associated with these risks, particularly as they pose material threats to the financial health of issuers, only appear to grow over time.

Strengthening the information provided by issuers regarding relevant cybersecurity risk management, strategy, governance, and incident reporting would provide investors with critical understanding of issuer cyber-resiliency while allowing investors to better assess and compare cybersecurity-related risks across companies. We also expect that the disclosures proposed in the Release will help investors identify and more accurately price cybersecurity-related risks, improving price discovery and allowing investors to more effectively direct financial capital to its highest-value use. We also note that cybersecurity risk information could provide investors with an important window into the overall quality of a company's broader risk management and oversight capabilities. Conversely, the absence of such

[3] https://www.sec.gov/about.shtml
[4] https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.
[5] https://www.sec.gov/rules/interp/2018/33-10459.pdf.
[6] Proposed Rule at 12.
[7] William Carter and Denise Zheng, "The Evolution of Cybersecurity Requirements for the U.S. Financial Industry," Center for Strategic and International Studies (July 2015), https://bit.ly/3TwPfFA, at 1.
[8] Proposed Rule at 57-59.
[9] *See, e.g.,* Proposed Rule at 5-11.

information could shield the true financial, operational, legal, and reputational impacts of mismanagement of cybersecurity risks.

By establishing a strong base of foundational information on cybersecurity risk and incident reporting, the Proposed Rule further seeks to reduce information asymmetries between issuers and investors as well as ensure *all* investors have access to the same fundamental data, leveling the playing field between large institutional shareholders and Main Street investors that are not large enough to demand or otherwise access individualized disclosure.

Finally, we note that many of the key aspects of the Proposed Rule are consistent with the recommendations made by members of the Investor as Owner Subcommittee in a 2017 Discussion Draft on cybersecurity and risk disclosure,[10] further underscoring the relative consistency in investors' demands for cybersecurity-related information.

Recommendation

The IAC supports the Proposed Rule and believes it serves the best interests of investors, representing a relatively modest effort that judiciously and appropriately builds on prior Commission efforts to improve issuers' disclosures on cybersecurity risk management and mitigation.

IAC Support for Key Aspects of the Proposal

Beyond providing broad support for the Proposed Rule, we highlight the following key aspects of the proposal that we view as particularly consequential in helping investors better understand and assess the quality of a firm's cybersecurity risk management and mitigation capabilities and performance.

Incident Disclosure

- **We support amending Form 8-K to require disclosure about material cybersecurity incidents within four business days after the registrant determines that it has experienced a material cybersecurity incident.** Investors need timely disclosure of a cybersecurity incident, along with sufficient information about an incident to allow investors to understand and assess the impact of the incident on the issuer's future prospects and facilitate price discovery. We believe the Proposed Rule generally satisfies investors' needs in this regard.

  We observe that investors often do not receive timely information about cybersecurity breaches from issuers. One comment letter responding to the Proposed Rule notes that an issuer waited

[10] *See* "Discussion Draft Re: Cybersecurity and Risk Disclosure," Investor as Owner Subcommittee, SEC Investor Advisory Committee (Dec. 2017), https://www.sec.gov/spotlight/investor-advisory-committee-2012/discussion-draft-cybersecurity-disclosure-iac-120717.pdf (Recommending certain enhancements to cybersecurity disclosure requirements, including (1) a more comprehensive description of company-specific risks; (2) specific, non-proprietary and non-sensitive information about past cyber-attacks, including summary information derived from root-cause analyses; (3) a general description of the issuer's efforts to minimize cybersecurity risks and its capacity to respond to cyberattacks, including information about internal governance; and (4) information on whether any member of the issuer's governing body, such as the board of directors, has experience, education, or expertise in cybersecurity, and if not, why a company believes that such board-level resources are not necessary for the company to adequately manage cyber risks.)

11 weeks to disclose a massive breach of over 383 million customer records in 2018, "exposing at least 25 million passport numbers and 8 million payment cards."[11] The same issuer experienced serious cybersecurity incidents in 2020 and 2022; neither incident was reported in an 8-k,[12] and the most recent incident – in July 2022 – was first made public via an anonymous email sent to a data security blog before it was confirmed by the issuer.[13]

We also support the Proposed Rule provisions that issuers provide periodic updates on previously disclosed cybersecurity incidents. As representatives of investors – including investors who routinely hold stocks for longer periods of time – we are particularly concerned about the potential harm to investors from ongoing security threats stemming from a prior cybersecurity incident. For example, threat actors continue to leverage the Log4j zero-day vulnerability in waging cyberattacks[14] while the full impact of the SolarWinds Orion hack may take several years to fully assess. The Commission's recommendation clarifies the disclosure rules around past incidents and ensures investors will have access to ongoing information about incidents as they evolve and the impacts of these incidents come into clearer view.

[11] Letter from Shivaram Rajgopal, Columbia Business School, and Alex Sharpe, Sharpe Consulting LLC, to the U.S. SEC re: File No. S7-09-22, "Comments on the SEC's Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure" (May 9, 2022), https://www.sec.gov/comments/s7-09-22/s70922-20128410-291323.pdf ("Marriott waited 11 weeks to reveal that 383 million customer records had been compromised, exposing at least 25 million passport numbers and 8 million payment cards….The data breach was noticed on September 8, 2018. Marriott filed the 10-Q covering the period ending September 30, 2018 on November 6, 2018. Although Marriott devoted two full paragraphs to the threat of cyberattacks in this filing, there is no mention of the massive data breach nor any disclosure of any economic impact to the company. Marriott then filed a form 8-K on November 30, 2018, disclosing the cyber-attack….[W]hen Senator Mitt Romney resigned from the board of Marriott on November 8, 2018, a Form 8-K was filed on November 9, 2018.").

[12] Marriott did publish a press release following the 2020 breach which included language suggesting that Marriott did not view the costs associated with the incident as "significant." *See* "Marriott International Notifies Guests of Property System Incident," (March 31, 2020), https://bit.ly/3BCd2N2 ("Marriott carries insurance, including cyber insurance, commensurate with its size and the nature of its operations, and the company is working with its insurers to assess coverage. The company does not currently believe that its total costs related to this incident will be significant.").

[13] *See* Carly Page, "Hotel giant Marriott confirms yet another data breach," TechCrunch+ (July 6, 2022), https://techcrunch.com/2022/07/06/marriott-breach-again/; and "EXCLUSIVE: Marriott hacked again? Yes. Here's what we know," DataBreaches.net (July 5, 2022), https://www.databreaches.net/exclusive-marriott-hacked-again-yes-heres-what-we-know/.

[14] For example, APT Lazarus Group - a state-sponsored cybercrime group - exploited vulnerabilities in VMWare Horizon to gain entry into the enterprise networks of energy companies based primarily in the U.S., Canada, and Japan for the purposes of "establishing long term access and subsequently exfiltrating data of interest to the adversary's nation-state." Jung soo An, Asheer Malhotra, and Vitor Ventura, "Lazarus and the tale of three RATs," Cisco Talos (September 8, 2022), https://blog.talosintelligence.com/2022/09/lazarus-three-rats.html.

Risk Management, Strategy, and Governance Disclosure

- **We strongly support the provisions of proposed Items 106 and 16J that would require an issuer to (1) describe its policies and procedures, if any, for the identification and management of risks from cybersecurity threats, including whether the issuer considers cybersecurity as part of its business strategy, financial planning, and capital allocation; and (2) require disclosure about the board's oversight of cybersecurity risk and management's role and expertise in assessing and managing cybersecurity risk and implementing the registrant's cybersecurity policies, procedures, and strategies.**

  We find the requirement to provide more information about the board's oversight of cybersecurity and the role management plays in assessing and managing risk to be helpful to investors given that cybersecurity is a corporate governance issue where boards must hold the CEO accountable, face potential litigation or regulatory scrutiny. The requirement for issuers to describe their policies and procedures for the identification and management of cybersecurity risks is also helpful to investors, as it provides investors with a stronger understanding of a company's resiliency to cybersecurity incidents and broader risk management capabilities without compromising the company's cybersecurity defenses.

  In voicing our support for these provisions, we note that the Proposed Rule does not require issuers that do not have any cybersecurity policies or procedures to disclose any information under proposed Items 106 and 16J. While we would be surprised to learn that a publicly-traded company lacks any internal infrastructure to manage and mitigate cybersecurity risks, in light of the urgency and unique nature of cybersecurity risks and incidents, we submit that the vast majority of investors – along with the members of the IAC – would view the complete absence of cybersecurity risk governance as overwhelmingly material to investment decision-making. We therefore recommend that issuers that have not developed any cybersecurity policies or procedures be required to make a statement to that effect.

IAC Recommendations to Further Enhance the Proposed Rule

We also submit the following recommendations that we believe would strengthen the Proposed Rule.

- **Require companies to disclose the key factors they use to determine the materiality of a cybersecurity incident in a periodic filing (such as a 10-K), as well as in an issuer's 8-K disclosure following a reportable cybersecurity incident under the Proposed Rule.** We suggest including this disclosure requirement among the disclosures mandated under proposed Item 106(b), regarding cybersecurity risk management and strategy. This will help improve the ability for investors to ensure comparability as they assess risk and historical attack prevalence across companies, while mitigating concerns from investors that companies may continue to underreport cybersecurity incidents under the Proposed Rule, should the Commission finalize it in its current form.

  Similarly, we are concerned that without clear guidance from the Commission, an issuer may fail to report cybersecurity incidents by misjudging the extent to which the incident is material to a

reasonable investor.[15] Though the Proposed Rule leaves the materiality determination to the issuer, we urge the Commission take any steps it deems necessary to mitigate any confusion around the circumstances under which an issuer would be expected to report cybersecurity incidents to investors.

- **Extend certain provisions of proposed Item 106 to registration statements under the Securities Act and the Exchange Act.** As noted above, proposed Item 106 would require an issuer to provide investors with important information about their cybersecurity risk management and strategy, including applicable policies and procedures, board and management oversight of cybersecurity risk, and updated disclosure about cybersecurity incidents. However, registration statements filed by firms in connection with an initial securities offering under the Securities Act and the Exchange Act are not covered by the Proposed Rule, despite the explicit application of disclosure obligations regarding cybersecurity risks and incidents on registration statements in the Commission's 2018 Interpretive Guidance.[16] We recommend that proposed Item 106 apply to registration statements, to the extent practicable.

  We note that by the time a private company is prepared to offer securities for sale on public exchanges via an initial public offering ("IPO"), the company most likely has achieved the level of maturity and sophistication to successfully manage a relatively expensive and time-consuming process involving exacting underwriting and due diligence, and believes it is prepared to satisfy

[15] Both the 2011 Staff Guidance and 2018 Interpretive Release recognize the importance of the materiality determination through Securities Act Rule 408, Exchange Act Rule 12b-20, and Exchange Act Rule 14a-9. See Basic Inc. v. Levinson, 485 U.S. 224 (1988); and TSC Industries, Inc. v. Northway, Inc., 426 U.S. 438 (1976) (Information is considered material if there is a substantial likelihood that a reasonable investor would consider it important in making an investment decision or if the information would significantly alter the total mix of information made available.) The 2011 Staff Guidance also stated, "Registrants also should consider the antifraud provisions of the federal securities laws, which apply to statements and omissions both inside and outside of Commission filings. See Securities Act Section 17(a); Exchange Act Section 10(b); and Exchange Act Rule 10b-5." *Also see* SEC Comm. Allison Herren Lee, "Living in a Material World: Myths and Misconceptions about "Materiality"" (May 24, 2021), https://www.sec.gov/news/speech/lee-living-material-world-052421 ("Although dependent upon the views of the reasonable investor, materiality determinations are typically made in the first instance by management. In doing so, management may rely on a "gut" feeling, anecdotal interactions, and even their own experience as investors…Particularly with respect to materiality determinations and the content of SEC filings, management often relies extensively on the advice of legal counsel. Yet, lawyers and auditors can also get the decision wrong. As with managers, they may see materiality differently from investors….Lawyers and auditors, like managers, are asked to apply the "reasonable investor" test without necessarily having sufficient understanding of what investors want or expect. But there's more to it than that. Both lawyers and auditors have built-in incentives to agree with management, particularly on close cases. They have an economic and psychological incentive to want to retain positive relations with management. This can create a form of implicit bias or predisposition, causing auditors and lawyers to often expend efforts to support, rather than independently analyze, management's decisions.")

[16] See 2018 Interpretive Guidance at 7 ("Companies should consider the materiality of cybersecurity risks and incidents when preparing the disclosure that is required in registration statements….)" and 9 ("Securities Act and Exchange Act registration statements must disclose all material facts required to be stated therein or necessary to make the statements therein not misleading. Companies should consider the adequacy of their cybersecurity-related disclosure, among other things, in the context of Sections 11, 12, and 17 of the Securities Act, as well as Section 10(b) and Rule 10b-5 of the Exchange Act."). Interestingly, the Release does pose a question to commenters regarding whether the Proposed Rule provisions regarding cybersecurity policies and procedures under proposed Item 106(b) also should apply to registration statements. *See* Proposed Rule at 43.

ongoing regulatory requirements like filing periodic reports with the Commission. Pre-IPO status does not render a company immune to cybersecurity risks, nor does it protect the company from the consequences of underdeveloped, inadequate, or ineffective cybersecurity risk management and mitigation infrastructure. To the contrary, pre-IPO companies may face heightened risks: for example, threat actors are now threatening to release hacked material non-public information associated with significant securities transactions and stock valuations unless they are paid a ransom.[17]

Further, while the existing cybersecurity risk and incident reporting guidance would remain in place, should the Commission decline to finalize the Proposed Rule, it is unclear if the 2018 Interpretive Guidance would continue to apply to registration statements if the Proposed Rule is adopted. Additional clarity on this point in the final release would be useful.

- **Reconsider the requirement that issuers disclose certain information about the board of directors' cybersecurity expertise.** Investors elect members of the board of directors to serve as their representatives at the firm with a fiduciary duty to oversee management – including the management of strategy and risks – on their behalf.[18] It is thus imperative that investors have enough information to adequately assess the performance of individual directors as well as the collective skills, capabilities, and effectiveness of the entire board in discharging its responsibilities. Additionally, more comprehensive information about particular areas of board duties and oversight can provide shareholders with a "window" into the board's decision-making process sufficient to develop a reasonable assessment of the board's ability to serve investors' interests.[19]

  Cybersecurity risks are pervasive, and the consequences of poor risk management and oversight can be severe. As noted in the previous section, we strongly agree that investors should have sufficient information to reasonably assess the board's effectiveness in overseeing these risks. We also acknowledge that it can be challenging – though not impossible – for a director exercising Duty of Care to oversee risks connected with an area of business for which they may lack expertise. However, we believe that all directors should possess the requisite skills and expertise to be able to provide effective risk oversight over all material risks to the business,

[17] *See, e.g.,* Federal Bureau of Investigation Cyber Division Private Industry Notification, "Ransomware Actors Use Significant Financial Events and Stock Valuation to Facilitate Targeting and Extortion of Victims" (November 1, 2021), https://www.ic3.gov/Media/News/2021/211101.pdf (Alerting the private sector to targeted attacks from ransomware actors threatening to release MNPI to interfere with events that could impact a company's stock price and market valuation such as initial offerings or mergers and acquisitions, and providing recent examples of recent attacks).

[18] *See, e.g.,* Council of Institutional Investors, "Corporate Governance Policies" (last updated March 7, 2022), https://www.cii.org/files/03_07_22_corp_gov_policies.pdf ("The board has a fiduciary responsibility to oversee company performance and the management of strategy and risks….The board should (1) monitor a company's risk management philosophy and risk appetite; (2) understand and ensure risk management practices for the company; (3) regularly review risks in relation to the risk appetite; and (4) evaluate how management responds to the most significant risks.")

[19] For example, shareholders often use the information issuers report annually in proxy statements about executive compensation as a "window into the boardroom" to better assess a board's effectiveness in overseeing management. *See* KPMG Board Leadership Center, "Executive Compensation as a Window Into the Board Room," KPMG US (2016), https://bit.ly/3Q6Pggi.

including novel or emerging risks. As part of active oversight, boards need to address any knowledge gaps in this regard. We are concerned that the board director cybersecurity expertise disclosure requirements under Proposed Item 407(j) may result in cybersecurity risk oversight left to the near-exclusive purview of relatively few board members (or a single board member) with the level of specialized technological knowledge contemplated in the Release.[20]

Further, we observe that the Proposed Rule does not define "cybersecurity expertise," leaving the issuer to make the determination on a case-by-case basis.[21] The absence of a clear definition could be misleading to investors whose understanding of cybersecurity expertise may substantively differ from the issuer's, while making it more difficult for an investor to compare risk oversight effectiveness across firms.

Instead, we believe that the provisions of the Proposed Rule relating to cybersecurity risk management, strategy and governance – including disclosing of the board's oversight of cybersecurity risk, identifying the board committee that is responsible for cybersecurity risk oversight, if applicable, and providing a description of management's role and competency in assessing and managing cybersecurity risk as provided in Proposed Item 106(c) – would provide investors with more effective and actionable insights into a board's skill and effectiveness in this regard.

As noted by the National Association of Corporate Directors ("NACD") in its written comments on the Release:

> The question of oversight and the question of expertise are different. A strong framework for oversight can make up for the lack of specialized expertise on the board, because outside expertise can be obtained and consulted by the board; however, the converse is not true. The presence of a cybersecurity expert on a board cannot make up for poor oversight processes, and does not excuse the full board from its oversight duties in this matter.[22]

We agree, and thus recommend the Commission reconsider mandating disclosure of director cybersecurity expertise as presented under Proposed Item 407(j).

Finally, we address the omission of an allowance for modified or delayed incident reporting in the Proposed Rule, should such a modification or delay be requested by law enforcement.[23]

---

[20] Although the Proposed Rule does not prescribe a definition for cybersecurity expertise, the introductory text does list specific criteria issuers "should consider" in evaluating whether a director has cybersecurity expertise. *See* Proposed Rule at 45.

[21] Proposed Rule at 45 ("Proposed Item 407(j) would not define what constitutes "cybersecurity expertise," given that such expertise may cover different experiences, skills, and tasks. Proposed Item 407(j)(1)(ii) does, however, include the following non-exclusive list of criteria that a registrant should consider in reaching a determination on whether a director has expertise in cybersecurity….")

[22] https://www.sec.gov/comments/s7-09-22/s70922-20128342-291099.pdf

[23] The Release does address the issue of how to treat situations under which local and state authorities may seek to have an issuer delay an incident report but rejects permitting a delay, stating, "[I]t is our current view that the importance of timely disclosure of cybersecurity incidents for investors would justify not providing for a reporting delay." See Proposed Rule at 25.

In both the 2011 Staff Bulletin and 2018 Interpretive Guidance, the Commission stressed the importance of disclosing cybersecurity incidents to the extent that a reasonable investor would view the information as material to an investment and/or voting decision.[24] Further, the 2018 Interpretive Guidance does not include a law enforcement exception: although it acknowledges that a company may need to cooperate with law enforcement in an ongoing investigation, it is explicit in stating that "an ongoing internal or external investigation - which often can be lengthy - would not on its own provide a basis for avoiding disclosures of a material cybersecurity incident" although it may impact the scope of the disclosure.[25]

While it may be tempting to create allowances in the final rule to serve other interests – including those of law enforcement – we underscore the Commission's role in protecting its key constituency: investors. We view the incident reporting provisions of the Proposed Rule as reasonably striking a defensible balance between the interests of investors who require high-quality, decision-useful information about cybersecurity incidents to inform decision-making and the needs of issuers seeking to safeguard sensitive and/or proprietary data from would-be attackers. We also recognize and agree with the Proposed Rule's recognition of the systemic risks posed by cybersecurity incidents which could have "serious effects on critical infrastructure and national security."[26] In this regard, we urge the Commission to consult and coordinate with the Cybersecurity and Infrastructure Security Agency ("CISA"), including during the rule-making process associated with the adoption of the Cyber Incident Reporting for Critical Infrastructure Act of 2022.

[24] *See, e.g.,* 2011 Staff Guidance ("The federal securities laws, in part, are designed to elicit disclosure of timely, comprehensive, and accurate information about risks and events that a reasonable investor would consider important to an investment decision…. In addition, material information regarding cybersecurity risks and cyber incidents is required to be disclosed when necessary in order to make other required disclosures, in light of the circumstances under which they are made, not misleading.") and 2018 Interpretive Release ("Companies should consider the materiality of cybersecurity risks and incidents when preparing the disclosure that is required in registration statements under the Securities Act of 1933 ("Securities Act") and the Securities Exchange Act of 1934 ("Exchange Act"), and periodic and current reports under the Exchange Act….Although these disclosure requirements do not specifically refer to cybersecurity risks and incidents, a number of the requirements impose an obligation to disclose such risks and incidents depending on a company's particular circumstances."

[25] 2018 Interpretive Guidance at 12.

[26] Proposed Rule at 8.