SOCIETY *for* Corporate Governance

May 9, 2022

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

RE: Comment Letter on Proposed Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, SEC File Number S7–09–22

Dear Ms. Countryman:

The Society for Corporate Governance ("Society") submits this letter in response to the request for public comments by the Securities and Exchange Commission ("SEC" or the "Commission") on the proposed rulemaking, "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," as announced by the Commission on March 9, 2022, and published in the Federal Register on March 23, 2022, at 87 FR 16590, File Number S7-09-22.

Founded in 1946, the Society is a professional membership association of more than 3,500 corporate and assistant secretaries, in-house counsel, outside counsel, and other governance professionals who serve approximately 1,600 entities, including 1,000 public companies of almost every size and industry. Our members play an active role in advising public companies on their cybersecurity disclosures and in responding to investor questions on this topic.

Executive Summary

We understand and appreciate the SEC's interest in setting rules regarding disclosure of cybersecurity incidents. Following the Commission's prior guidance, corporations began establishing internal disclosure controls and procedures for determining when to disclose certain cybersecurity incidents. We welcome the use of the materiality standard for cybersecurity incident reporting, but we have concerns about other aspects of the proposed rule.

In particular, the Society believes that the definition of "cybersecurity incident" is overbroad in that it includes those in which there has not been any injury or measurable impact

to date, and that it would require disclosure based on speculation as to the materiality of any such incident. We also believe that the lack of a feasible law enforcement or national security exception for disclosures is problematic, and that the proposed disclosure timing is unworkable. We are concerned that premature disclosure before a company fully understands the scope of (and has had an opportunity to remediate) a cybersecurity incident could enable malicious actors in carrying out additional attacks. We also believe that the burden of the proposed periodic incident reporting would outweigh any potential benefit to investors. Finally, the Society is concerned about the Commission's proposal for expansive disclosures about risk management, strategy, and governance. Among other things, the proposed rule will pressure issuers to appoint a technical cybersecurity expert to their boards, regardless of whether it is appropriate for their particular governance needs. We also note that many of the proposed disclosures in this area are unique among SEC rules and carry with them unintended consequences the Commission and market participants may not have fully considered.

We encourage the SEC to revise this proposed rule as follows so that investors receive more complete decision-useful information from issuers about material cybersecurity incidents: 1) narrow the definition of reportable cyber incidents to include only those that cause injury or a material impact; 2) allow companies to delay disclosure so they don't interfere with law enforcement or national security investigations; 3) adjust the disclosure framework to reflect state notification statues, the complexity of assessing the materiality of cyber incidents, and the need for issuers to remediate vulnerabilities before public disclosure; 4) protect companies from the costs of frivolous securities litigation by providing a safe harbor and/or allowing "furnished" incident disclosures; 5) not require issuers to speculate on the cumulative impact of previously disclosed cybersecurity incidents; and 6) allow greater flexibility for companies to explain how their boards and management teams oversee and manage cybersecurity risks.

I. The Definition of "Cybersecurity Incident" Is Overbroad and Would Require a Speculative Materiality Assessment.

A. The Society Supports the Materiality Standard.

We support the SEC's proposal to use "materiality" as the standard for disclosures of cybersecurity incidents. The "materiality" standard is well-known to issuers and investors and reflects the balancing of investor interests and the important needs of public companies. Restricting the reporting obligation to "material" incidents is necessary given that any filing related to a cybersecurity incident is likely to attract a great deal of attention and may cause an inflated reaction from the market. We do not expect these materiality assessments to be easy – and we discuss particular challenges regarding assessing the materiality of incidents that have

not caused injury or measurable impact to date, and timing considerations, below – but we do agree that "materiality" is the correct standard.

B. The Proposed Definition of "Cybersecurity Incident" That "Jeopardizes" an Information System Alone Is Too Broad and Should Include Actual Loss.

The Society believes the proposed definition is problematic because the materiality analysis would require companies to consider a parade of possibilities, including by predicting the actions of malicious actors whose motivations and scope of action may not be known.

The proposed definition of "cybersecurity incident" as "an unauthorized occurrence on or conducted through an issuer's information system that jeopardizes" an issuer's information system or information is overbroad, because it includes incidents where no injury or measurable impact has occurred to date. Requiring issuers to publicly disclose incidents that materially "jeopardize" their information systems or information – "to expose to danger or risk"[1] – requires issuers to speculate in a manner that is counterproductive to providing useful information to the investing public and incompatible with the materiality analysis and may increase the risk from such incidents. Many cybersecurity incidents start with an observable occurrence in an information system that could allow malicious actors the ability to cause loss, steal data, or disrupt business operations. However, assessing whether a cybersecurity incident will (or will not) be material is nearly impossible when the question is whether it "jeopardizes" an information system, i.e., "expose[s an issuer] to danger or risk" instead of assessing whether it *actually has* caused loss, harm or failure, and if so in what amount. So, while it may be reasonable (albeit difficult) for issuers to assess the materiality of those cybersecurity incidents that have had an actual impact on an issuer's information systems or information, it is unreasonable to demand issuers evaluate materiality where an incident might only hypothetically impact such systems or information.

C. Disclosure Required by the Overbroad Definition of Cybersecurity Incident May Be Alarming and Potentially Dangerous.

There is no uniform definition of "jeopardize" that would be free of speculation and subject to reasonable, objective agreement, and these speculative assessments will suffer from uncertain information and look completely different when judged with the benefit of hindsight. So, faced with the SEC's proposed definition, many issuers will err on the side of public disclosure because it will be so difficult to determine the materiality of speculative scenarios in a short period that issuers may be concerned about securities liability for failing to disclose them. This premature disclosure could not only provide unduly alarming information to investors, but also may significantly increase the risk arising from the incident. Given the SEC's proposed

[1] *See* Merriam Webster at https://www.merriam-webster.com/dictionary/jeopardize.

Form 8-K disclosure requirements for cybersecurity incidents, disclosure may be required before the risk can be remediated, giving malicious actors the identity of a vulnerable company, setting it up as an easy target.

The Commission appears to be sensitive to these concerns because the proposed rule excludes from the definition of "cybersecurity incident" the category of cybersecurity *vulnerabilities* – flaws that are inherent to systems or software, rather than caused by unauthorized intrusions. The SEC did not propose that such vulnerabilities be disclosed, even if a potential exploit of them would be material,[2] presumably because of the substantial risks of requiring disclosure before the vulnerability can be addressed. In other words, a vulnerability could be described as putting at risk an information system — i.e., jeopardizing it — without that risk coming to fruition, but it is not covered by the proposed rule. The Commission should take the same approach with respect to cybersecurity incidents that have not to date done any more than jeopardize such systems.

D. Relying on NIST and PPD-41 Is Inappropriate as Those Regulatory Definitions Do Not Address Public Disclosure.

The Society also questions the Commission's reliance on definitions from the National Institute of Standards and Technology ("NIST") and the Presidential Policy Directive 41 ("PPD-41") as the basis for the SEC's approach to cybersecurity disclosure, as those definitions include actual harm and do not address public disclosure. The SEC states in footnote 80 that it derived the proposed rule's definition of "cybersecurity incident" from NIST and PPD-41. However, the proposed rule's definition omits important terms that appear in each of those source definitions. In particular, NIST defines a "cybersecurity incident" as:

> *An occurrence that (1)* ***actually or imminently jeopardizes****, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.*[3]
> (emphasis added)

[2] Two examples of material vulnerabilities are the critical vulnerabilities discovered in modern computer processors, announced in 2018, named "Meltdown" (CVE-2017-5754) and "Spectre" (CVE-2017-5753 and CVE-2017-5715). CISA, Meltdown and Spectre Side-Channel Vulnerability Guidance, Alert TA18-004A (Jan. 4, 2018), https://www.cisa.gov/uscert/ncas/alerts/TA18-004A. According to CISA, "Spectre affects almost all devices including desktops, laptops, cloud servers, and smartphones."

[3] NIST, Computer Security Resource Center Glossary: "Cybersecurity Incident" (last visited Feb. 6, 2022), available at https://csrc.nist.gov/glossary/term/cybersecurity_incident (emphasis added).

Similarly, PPD-41 defines a "cybersecurity incident" as:

> *An event occurring on or conducted through a computer network that* ***actually or imminently jeopardizes*** *the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon. For purposes of this directive, a cyber incident may include a vulnerability in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.*[4]

And PPD-41 further defines a "significant cyber incident" as:

> *A cyber incident that is (or group of related cyber incidents that together are)* ***likely to result in demonstrable harm*** *to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.* (emphasis added)

By placing "actually or imminently" before "jeopardizes," both NIST and PPD-41 clearly contemplate that a cybersecurity incident is something more than an event that merely "jeopardizes" an information system. Additionally, PPD-41 takes this concern one step farther by clarifying in its definition that events are only "significant" if they are "likely to result in demonstrable harm." Careful reading of these sources, therefore, would support a more concrete definition than the SEC's proposed definition, which sweeps speculative risks into the calculus when determining what requires public disclosure.

Using a standard that requires an actual impact to information systems or systems would be consistent with other federal requirements. In 2022, when establishing cyber incident reporting requirements for critical infrastructure, Congress defined "cyber incident" as an occurrence that actually jeopardizes information or an information system.[5] Similarly, in setting the regulatory notification standard for banking entities and their service providers, the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation recently defined "computer-security incident'' by modifying the NIST definition to limit it to "an occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the

[4] Presidential Policy Directive -- United States Cyber Incident Coordination (July 26, 2016) ("PPD-41") (emphasis added).

[5] *See* Consolidated Appropriations Act, 2022, H.R. 2471, 117th Cong. (2022) (Section Y: Cyber Incident Reporting for Critical Infrastructure Act of 2022) (hereinafter "CIRCIA"), § 2240(6) and 6 U.S.C. § 659(a)(5).

system processes, stores, or transmits."[6] In both instances, the federal legislation or regulation has further limited those "incidents" that must be reported to the federal government to those that are significant.[7] Thus, the federal government is in agreement that the absolute floor for potentially reportable cybersecurity incidents is those that have actual impact to information or an information system.

Using NIST and PPD-41 to define when issuers must publicly disclose cybersecurity incidents conflates two unrelated contexts and is unworkable in practice. It would be more appropriate for the Commission to adopt a definition whereby "cybersecurity incident" is defined as "an unauthorized occurrence on or conducted through an issuer's information system that actually compromises the confidentiality, integrity, or availability of an issuer's information system or information residing therein." This definition — drawn directly from data breach statutes — provides a more concrete definition for cybersecurity incident, on which a materiality analysis (albeit difficult) is feasible.

Even if we could read these sources in a way that supports the Commission's proposed definition, NIST and PPD-41 are fundamentally the wrong standards on which to base a rule defining the contours of when issuers must *publicly disclose* material cybersecurity incidents. There is nothing in NIST that prescribes when incidents must be disclosed, because that is not its purpose. NIST is a framework that supports *internal* cybersecurity risk management and response. It makes sense, therefore, that NIST defines "cybersecurity incident" broadly. Risk management programs should consider all kinds of cyber risks and to help design controls to address them.

Similarly, PPD-41 sets forth principles governing how the federal government will coordinate response to cybersecurity threats to the federal government, national security, and the economy. Again, it makes sense to define terms broadly, because the directive seeks to apply these same principles to all kinds of cyber risks. But the PPD-41 is merely a framework for incident response and coordination. There is nothing in the directive that mandates when cybersecurity incidents must be disclosed, let alone publicly disclosed. To the contrary, PPD-41 recognizes that private sector information can be sensitive and thus this directive provides:

> *To the extent permitted under law, Federal Government responders will safeguard details of the incident, as well as privacy and civil liberties, and sensitive private sector information, and* ***generally will defer to affected entities***

[6] *See, e.g.*, 12 C.F.R. § 53.1 (emphasis added); *see* 86 F.R. 66425 n.3

[7] CIRCIA at § 2240(4); 86 F.R. 66425 (limiting reporting to an incident that "disrupts or degrades, or is reasonably likely to disrupt or degrade, the viability of the banking organization's operations, result in customers being unable to access their deposit and other accounts, or impact the stability of the financial sector").

in notifying other affected private sector entities and the public. *In the event a significant Federal Government interest is served by issuing a public statement concerning an incident, Federal responders will coordinate their approach with the affected entities to the extent possible.* (emphasis added)

E. Disclosing Unrealized Risks May Negatively Impact Contracts With Third Parties.

If the rule were to require disclosure about unrealized risks, the rule could negatively impact existing information flow between issuers and their customers, vendors, and service providers. Contracts for cybersecurity-sensitive goods and services typically contain customized security disclosure requirements. These provisions are usually carefully considered, with the threshold and timing of disclosure to customers and other third parties as important negotiated terms. These contractual requirements typically only require disclosure where there has been actual impact to the customer's data or where such impact is reasonably likely.[8] Similarly, as referenced above, laws and regulations aimed at protecting privacy and security sometimes require disclosure of incidents at third-party vendors or service providers but, again, are typically triggered only where there is a reasonable likelihood that actual loss has already occurred.[9]

---

[8] Various cloud computing providers have adopted breach notification contract terms that limit those notifications to incidents that involve an impact on data or information. *See, e.g.*, Google's Data Processing and Security Terms provide that "Google will notify Customer promptly and without undue delay after becoming aware of a Data Incident", with "Data Incident" defined as "breach of Google's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data on systems managed by or otherwise controlled by Google." Google, Data Processing and Security Terms (Customers), https://cloud.google.com/terms/data-processing-terms (last visited Apr. 27, 2022).
IBM's Data Security and Privacy Principles provide that "IBM will notify Client without undue delay upon confirmation of a Security Incident that is known or reasonably suspected by IBM to affect Client" and "Security Incident is defined as "unauthorized access and unauthorized use of [data, software, and information that Client or its authorized users provide, authorize access to, or input to IBM Services]." IBM, IBM Data Security and Privacy Principles, 1, 3, https://www.ibm.com/support/customer/csol/terms?id=Z126-7745&lc=en#detail-document (last visited April 27, 2022).
Microsoft's Online Services Data Protection Agreement provides for customer notification where "Microsoft becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data or Personal Data while processed by Microsoft." Microsoft, Microsoft Products and Services Data Protection Addendum, 9 (Sept. 15, 2021), https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA.
Oracle's Data Processing Agreement for Oracle Services specifies that "Oracle will notify you of a confirmed Personal Information Breach without undue delay but at the latest within 24 hours" and defines "Personal Information Breach" as "a breach of security leading to the misappropriation or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Information transmitted, stored or otherwise Processed on Oracle systems or the Services environment that compromises the security, confidentiality or integrity of such Personal Information." Oracle, Data Processing Agreement for Oracle Services, 4-5 (June 26, 2019), https://www.oracle.com/a/ocom/docs/corporate/data-processing-agreement-062619.pdf.

[9] Many state data breach notification laws define a notifiable "data breach" in a manner that requires access or acquisition of personal information. *See, e.g.*, Cal. Civ. Code § 1798.82(g) (defining "breach of the security of the

If the SEC's rule is enacted as proposed, issuers concerned about securities liability may be incentivized to demand additional information about risks at third parties, either by revising their contracts, or by requesting additional information during unfolding cybersecurity incidents (or about past incidents). We do not believe these additional efforts to obtain information would be broadly beneficial. The need of investors to know about risks involving third parties that have not to date caused any injury or measurable impact is tenuous at best, and the downside of this requirement is the disruption caused by issuers seeking such information, information that goes beyond what they otherwise would deem necessary to run their business or serve their customers and what lawmakers and regulators seeking to protect security and privacy have deemed appropriate. If issuers obtain additional information about cybersecurity risks at third parties, another potential cost arises: the pressure to provide their own customers remedies for this unexploited and remote risk – for instance, by providing credit or other monitoring services – that no one but the SEC has deemed important enough to make subject to reporting requirements.

II. The Proposed Rule Lacks a Feasible Law Enforcement/National Security Exception.

The Society believes that the proposed rule must allow an issuer to delay disclosure based on a request from law enforcement or national security agencies, and the SEC's proposed exception is unworkable. The SEC's failure to accommodate law enforcement and national security concerns is incongruous with existing cyber incident notification requirements at the state and federal level and would undermine national, corporate, and personal security interests. While the SEC has stated that, on balance, the importance of timely disclosures for investors does not justify reporting delays to facilitate law enforcement investigations, the Society believes that investors would be better served by allowing companies to delay disclosure when requested by law enforcement or national security officials. Premature disclosure of a cybersecurity incident amid a law enforcement/national security investigation likely will cause an adverse market reaction and greater share price volatility as investors try to make investment decisions based on incomplete information that likely will change as more facts are made public by law enforcement or security officials.

Data breach notification laws at the federal and state level that require public disclosures of cybersecurity incidents allow for a delay in such reporting to account for the needs of law

---

system" as "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business"); N.Y. Gen. Bus. Law § 899-aa(1)(c) (defining "[b]reach of the security of the system" as "unauthorized access to or acquisition of, or access to or acquisition without valid authorization, of computerized data that compromises the security, confidentiality, or integrity of private information maintained by a business"); Tx. Bus. & Com. Code § 521.053(a) (defining "breach of security system" as "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person").

enforcement or national security. As a federal example, the Health Insurance Portability and Accountability Act ("HIPAA"),[10] under rules set by the U.S. Department of Health and Human Services, requires notification to individuals within 60 days of a security event impacting their protected health information and allows for a delay if notification would impede a criminal investigation or cause damage to national security. This concept is also found in state data breach notification laws, which allow for the delay of notification of a breach based on a request of law enforcement.[11] Furthermore, disclosing information covering cybersecurity incidents implicating classified information is prohibited under federal law and incidents involving classified information already are subject to strict, nonpublic reporting requirements to relevant government agencies. We presume the SEC's proposed rule was not intended to imply that classified information should be disclosed, and we believe there should be an express exception.

The SEC has invited commentors to weigh in the possibility of adding an exception based on written notification from the U.S. Attorney General that national security requires delay in disclosure. We believe that such a narrow exception would not be sufficient to address issuers' concerns, for the following reasons:

- The SEC's question reflects that it is solely concerned with the issue of national security. While national security is plainly a sufficient consideration for delaying disclosure, it is not the only one. There are a variety of legitimate law enforcement needs that should also justify delayed disclosure, including because certain cybersecurity incidents could pose a threat to human or facility safety.

- Even if the exception were appropriately limited to national security, the Attorney General's office is not the only government entity that should be consulted in assessing the risks of disclosure. For example, Defense Federal Acquisition Regulation Supplement requirements established by the Department of Defense ("DOD") requires relevant entities to report security events to the DOD directly.[12] The Cybersecurity & Infrastructure Security Agency ("CSIA") was recently designated by Congress as the ingestion point for required security event reporting by critical infrastructure entities.[13] CISA is then tasked with distribution of such information to relevant federal departments and agencies, including specifically those that "identify and track ransom payments, including those utilizing virtual

[10] 45 C.F.R. § 164.412.

[11] *See, e.g.*, Cal. Civ. Code § 1798.82(c); N.Y. Gen. Bus. Law § 899-aa(4); Tx. Bus. & Com. Code § 521.053(d).
[12] 48 C.F.R. § 252.204-7012(c).

[13] Consolidated Appropriations Act, 2022, H.R. 2471, 117th Cong. (2022) (Section Y: Cyber Incident Reporting for Critical Infrastructure Act of 2022) (hereinafter "CIRCIA"), § 2242.

currencies." CISA has publicly acknowledged that it "always ensur[es] that cyber incident reporting received by [CISA] is immediately shared with [our FBI teammates]."[14] It is worth noting that these federal reporting requirements are non-public disclosures and are exempt from government disclosure requirements like the Freedom of Information Act. To encourage voluntary reporting for purposes of national security, critical infrastructure reporting to CISA cannot be used by any federal, state, local, or tribal government to regulate or pursue enforcement against the reporting entity. By contrast, under the SEC's proposal, the FBI would likely be provided with information about many cybersecurity incidents around the same time it would become publicly available via a Form 8-K, without any of the safeguards CISA provides. This could frustrate federal law enforcement's efforts to investigate and apprehend the malicious actors behind cybercrime and provide less support to victimized companies and their shareholders.[15]

- In certain industries such as critical infrastructure and aerospace and defense, companies may be contractually or even legally precluded from making a proposed public disclosure of a cyber incident due to national security concerns unrelated to an ongoing law enforcement investigation. The SEC's cybersecurity rule should thus also authorize the Department of Defense, the Department of Homeland Security, and U.S. intelligence agencies, in addition to the Department of Justice, to issue national security determinations that would allow companies to delay disclosure. This change would avoid these companies being placing in the untenable position of having to choose between making a timely SEC disclosure or facing potential civil or criminal liabilities for making such a public disclosure.

- Given the four-business day Form 8-K deadline after determining materiality, we believe it would be impossible to obtain such a written national security determination from the Attorney General or other high-level agency officials in advance of that deadline.

In light of the potential harm to national security or law enforcement investigations that could result from premature public disclosure, we encourage the SEC to delay implementation of

[14] *See* Jen Easterly (@CISAJen), Twitter (March 4, 2022, 9:53 AM), https://twitter.com/CISAJen/status/1499805121437487108.

[15] Under the current "Shields Up" Advisory from CISA regarding potential cybersecurity attacks relating to the Russian attacks on Ukraine, CISA is requesting that organizations report cyberactivity and events to CISA or the FBI urgently. CISA, Shields Up Technical Guidance, https://www.cisa.gov/uscert/shields-technical-guidance (last visited April 27, 2022). CISA and the federal government's ability to act on such information would likely be negatively impacted if issuers also had to publicly disclose details regarding such activity or events within days.

this rule until it has had the opportunity to coordinate reporting requirements with other federal agencies. The Cyber Incident Reporting Council, provided for in the recently passed Cyber Incident Reporting for Critical Infrastructure Act of 2022, will likely have suggestions for how to structure the public reporting requirements relating to cybersecurity incidents contemplated by the SEC. If the Commission is not willing to wait for this guidance, however, we encourage the SEC to permit a delay in public disclosure (or provide a regulatory safe harbor) for incidents where companies are asked to postpone disclosure by law enforcement or national security officials. Alternatively, the Commission should adopt the more flexible approach for disclosure timing described in the next section of this letter, which incorporates the interests of law enforcement and national security into an issuer's disclosure obligation.

III. The Proposed Incident Disclosure Timing Is Unworkable.

In addition to the concerns described above, we also have serious concerns with the Commission's proposed disclosure timing. Currently, the proposed rule requires that issuers disclose information about a cybersecurity incident via a Form 8-K filing within four business days after the issuer determines that it has experienced a material cybersecurity incident, with that determination to be made "as soon as reasonably practicable after discovery of the incident."

We believe that the proposed Form 8-K reporting requirement presents significant risks to both issuers and investors. We encourage the Commission to instead mandate disclosure only in required quarterly reports once the issuer has determined that a material incident is appropriate for disclosure. Using such disclosure timing would lessen the risk of unintended consequences from premature disclosures by not drawing undue attention to any particular incident, allow for a more comprehensive assessment of the severity and impact of cybersecurity incident, and enable issuers to contextualize these incidents within a broader disclosure framework.

If the SEC opts to impose a Form 8-K filing obligation for cyber incidents, we propose a more flexible approach based on state data breach notification laws that would more appropriately reflect the complexity of cyber incidents.

A. Analyzing Cyber Incidents Often Takes Substantial Time.

Cybersecurity incidents are complex by their very nature. The actual impact and effect of a cybersecurity incident is often not well known upon its initial discovery. Determination of the scope of a cybersecurity incident and its actual impact on the issuer's operations, information systems, or information requires substantial investigation, often including the engagement of third-party experts. Investigations can be particularly difficult in incidents where the evidence that the issuer may want to examine has been destroyed, obfuscated, or altered by the threat

actor.[16] Accordingly, in many circumstances, issuers will need substantial time – weeks or even months – to validate and confirm materiality determinations. This analysis is also occurring during a time when the information system experts needed to inform the determination are often also working actively to address the incident, important work that should be prioritized. Once a Form 8-K filing is public, investors, analysts, and other market participants likely will have follow-up questions about the incident, presenting an additional distraction for these experts.

An understanding of an incident and its consequences often changes substantially in the first days or weeks after discovery. Issuers will struggle to determine when they know enough, particularly as there is often additional information to be analyzed that will provide detail about actual impact and severity of a cybersecurity event. Additionally, as the investigation proceeds there is often information that needs to be reconciled or deconflicted, and theories of impacts and how the systems were compromised often also change dramatically. For example, it is common for there to be an operating premise early on in an investigation that, after further investigation, is proved wrong. Sometimes, an incident initially may seem far worse than it turns out to be. Other times, incidents that initially appear to be relatively minor turn out to be more significant.[17] During their investigations, issuers sometimes also reach out to benchmark with peers, formally or informally, sharing tentative views and theories.

The SEC may believe that beginning the four-day Form 8-K clock after an issuer concludes an incident is material would be sufficient to address issuers' concerns. However, Society members disagree, particularly given the SEC's additional directive that the materiality conclusion be reached "as soon as reasonably practicable." Such a requirement would put pressure on an issuer to draw a conclusion about an incident early on, to avoid any claim (made worse by hindsight bias) that the issuer could or should have known about an incident's materiality sooner. Indeed, issuers with mature cybersecurity programs that include sophisticated monitoring may be aware of *more* cybersecurity incidents than companies with newer cybersecurity programs with less effective monitoring. Issuers with more mature programs are also likely to have earlier analyses of and communications about cybersecurity incidents that could form the basis for disclosure. This is likely to be true, even though these issuers with mature programs may have fewer material incidents by virtue of their monitoring efforts. For this

[16] According to a 2021 survey of 500 security and risk leaders at large organizations, counter incident response measures, such as log deletion, are seen in 63% of incidents. Kroll, Red Canary, and VMware Carbon Black, "The State of Incident Response 2021," 4, available at https://www.vmware.com/resources/security/the-state-of-incident-response-2021.html.

[17] For example, Okta was criticized for its perceived delay in telling its customers about a security event that occurred at one of its vendors. After confirming that the vendor event potentially impacted several hundred Okta customers, Okta said that it "did not know the extent of the [vendor] issue" at the time of the vendor's initial disclosure and "didn't recognize that there was a risk to Okta and our customers." Liam Tung, ZD Net, "Okta: We made a mistake over Lapsus$ breach notification" (March 28, 2022), https://www.zdnet.com/article/okta-we-made-a-mistake-over-lapsus-breach-notification/.

reason, the SEC's proposed timing may single out for additional enforcement scrutiny the very issuers that are working the hardest to find and remediate incidents. These companies may respond by providing protective disclosures about well-managed incidents that would not be helpful for investors, and could, potentially, provide the misimpression that investing in that company is riskier than those with less robust cybersecurity programs. As noted earlier in this letter, these early disclosures may also subject companies to attacks from other malicious actors.

Ransomware attacks demonstrate another type of risk from early disclosure. Ransomware attackers frequently make sweeping claims about their access to company systems and data that can take significant time to investigate. But early disclosure of a ransomware attack before recovery of systems and data could signal to the attacker the extent to which the attack has impacted the issuer either operationally or in relation to data impacted and allow the attacker additional leverage to increase its extortion demands. Beyond the initial ransomware attacker, a disclosure could create additional demand in the illegal market for data exfiltrated from the issuer and allow for exploitation of exfiltrated data before an issuer is able to notify individuals whose data was impacted in the incident.

Another common cybersecurity incident scenario where early disclosure would be particularly harmful involves incidents initiating at third-party entities. The issuer may need to obtain information from the third party to support the investigation and allow for an accurate disclosure. But the third party may not have disclosed the incident itself, either because it is not subject to any SEC disclosure requirements, or because it does not believe the incident is material to them. Obtaining such information from third parties can be difficult and prolong the time it takes to develop an accurate understanding of the incident and its potential or actual impact on the issuer. At some point, however, an issuer may conclude that it can wait no longer to disclose, even with imperfect information. This may not only result in the issuer providing information about an incident that is not actually material, thus causing unnecessary investor concern, but also may reveal confidential information about an issuer's supplier relationships that may create a risk of future harm to the company in a security or general business context.

In sum, a four-day disclosure timeline would not allow time for deliberate examination and (as necessary) reexamination of the available evidence that would confirm a materiality determination, potentially leading to a premature and inaccurate disclosure of the actual impact of a cybersecurity incident.

For all the reasons described above, we believe the SEC's proposed incident disclosure rules could: (1) unduly distract issuers from important remediation efforts; (2) discourage information sharing and other early analyses; (3) provide malicious actors with information they can use to cause harm; (4) cause a disproportionate reaction from investors, as well as customers and suppliers, about incidents that, in the end, turn out not to be significant; and 5) prompt some

investors to make investment decisions before an issuer has completed its full assessment of an incident.

B. Disclosure Timeframes Should be Based on State Data Breach Statutes.

Rather than tying the Form 8-K disclosure obligation to an accelerated materiality determination conducted "as soon as reasonably practicable," we encourage the Commission to consider a reporting timeframe that reflects the complex nature of cybersecurity incidents.

We recommend that the SEC consider adopting a more flexible approach to the timing of disclosure. Borrowing from state data breach statutes,[18] this approach could require issuers to furnish a Form 8-K within four business days of confirming that a material[19] cybersecurity incident should be disclosed, based on the following priorities:

(1) an expedient disclosure, without unreasonable delay;
(2) allow for a delay in public disclosure when requested by law enforcement or government agencies focused on national security or the security of critical infrastructure;
(3) allow for measures necessary to determine the scope of the breach and restore the reasonable integrity of the impacted system(s) or data prior to public disclosure, and;
(4) allow for reasonable notification to individuals with impacted data.

These considerations better reflect the important interests that issuers should review when determining disclosure than the purely time-focused "as soon as reasonably practicable." They would allow the issuer to weigh the demands of a complex situation and the risks that advance disclosure creates and make any necessary disclosure in accordance with reasonable judgments around those competing goals. Such goals include, as already discussed, the needs of law enforcement and national security, the need to restore the integrity of information systems before disclosure, and the company's interest in not encouraging additional attacks by malicious actors. In essence, this multi-factorial test allows issuers to consider the appropriate priorities in timing their disclosure.

To address the SEC's potential concern that such a framework may provide issuers too much discretion, we note that the determination of whether an incident is "material" would be within an issuer's discretion under the Commission's proposed rule. Cybersecurity incident

[18] *See, e.g.*, Cal. Civ. Code § 1798.82(a); Idaho Code § 28-51-104; 815 Ill. Comp. Stat. § 530/10(a); Minn. Stat. § 325E.61(1)(a); N.J. Stat. § 56:8-163(a); and S.C. Code § 39-1-90(A).

[19] While state data breach laws typically allow more time for issuers to assess the severity of an incident and coordinate with law enforcement, some laws require companies to provide notification of incidents that are not material.

reporting will inherently require issuers to exercise considerable judgement, disciplined by the possibility of inquiry and enforcement action should the Commission not agree. The approach we propose would allow issuers to exercise that discretion based on the factors most important to the disclosure decision.

Finally, we encourage the SEC not to include these cyber incident disclosures on the list of Form 8-K items that could potentially cause loss of Form S-3 eligibility and to allow this new Form 8-K item be "furnished" rather than "filed" for liability purposes, given how difficult and unclear the appropriate timing of disclosure in this area inherently is.[20]

IV. New Periodic Reporting Requirements Would Not Be Meaningful to Investors.

The SEC's proposed requirements for periodic reporting about incidents (in Form 10-Qs, Form 10-Ks, and, for foreign private issuers, Form 20-Fs) also raise concerns.

First, we believe the requirement for issuers to provide material updates regarding previously disclosed incidents will prove difficult for issuers and provide limited, if any, value to investors. This is particularly true with respect to the proposed requirements that issuers disclose "any changes in the issuer's policies or procedures as a result of a cybersecurity incident, and how the incident may have informed such changes." The reasons for changes in a cybersecurity policies and procedures are multi-faceted and complex, and it would be extremely challenging for issuers to determine the relationship between those changes and any one incident. Especially given how qualified any disclosure in this area would have to be to be accurate, it is not clear how investors would benefit from such disclosure. This type of periodic disclosure also raises security concerns, as reported changes to cybersecurity policies and procedures after a cybersecurity incident could reveal potential roadmaps (details on what we have changed and why) to vulnerabilities or associated information systems.

Similarly, the requirement that an issuer disclose "any *potential* material future impacts on the [issuer]'s operations and financial condition" related to a previously disclosed incident is unlikely to add value to investors that exceeds the burden it would place on issuers or that would provide any useful supplement to existing disclosure obligations. Specifically, it is unclear what

[20] Given the inherent difficulty in assessing the materiality of cybersecurity incidents, we encourage the Commission to provide a reliance and liability safe harbor against Exchange Act Section 10(b) and Rule 10b5-1 private claims against companies over any failure to furnish a Form 8-K on a timely basis to disclose a cyber incident. The SEC took a similar approach in its 2004 guidance on Form 8-K, providing a limited safe harbor for 8-K filings to announce the entry or termination of material definitive agreements, material impairments, restatements, and other matters. *See* Final Rule, Additional Form 8-K Disclosure Requirements and Acceleration of Filing Date, Release Nos. 33-8400; 34-49424 (August 23, 2004).

value, if any, disclosure of *potential* future impacts on the issuer's operations and financial condition would give investors above the existing Item 303 disclosure requirement, which require issuers to disclose any future impacts *reasonably likely* to have a material effect on an issuer's financial condition or operating results.[21] Furthermore, issuers are already required to disclose in their periodic reports matters that could make their securities speculative or risky.[22]

Additionally, there are potential security impacts from required disclosure of the status of incident remediation. The disclosure of any details pertaining to remediation is inappropriate, especially before an incident has been remediated. In general, these details should not be disclosed as they could expose areas of vulnerability to current and other potential threat actors. Further, remediation is not well understood by, and could be misleading for, current and potential investors. More detailed reporting about remediation could cause issuers to report developments that could point malicious actors to vulnerabilities that can be exploited or cause undue alarm among investors. We also note that disclosing updates on remediation would burden those professionals who need to focus on completing remediation (i.e., there will be inevitable follow-up questions from investors, analysts, customers, news media, etc.).

Second, with respect to the SEC's proposal that issuers specifically disclose "when a series of previously undisclosed individually incidental immaterial cybersecurity incidents has become material in the aggregate," we believe issuers will struggle to understand the principles on which the SEC expects an issuer to consider in aggregating incidents and the period of time such aggregation should cover. In what respect must the incidents be similar? The proposed rule provides no real guidance, and we do not believe meaningful guidance would be possible, given how individualized cybersecurity incidents can be. The burden of gathering information and evaluating it from multiple possible SEC perspectives does not, in our view, justify any possible benefit to investors, especially given that any material risks that arise from cybersecurity must already be reported in existing risk factor disclosures.

V. The Proposed Rule's Risk Management, Strategy, and Governance Disclosures Are Counterproductive and May Diminish Board Effectiveness

The SEC's proposed rule includes detailed requirements for disclosure about risk management, strategy, and governance that we believe will be counterproductive to an issuer's cybersecurity programs, and to public company governance generally. In particular, adopting a "one size fits all" approach to disclosure about board and management governance of cybersecurity is unlikely to produce any more useful information for investors than they can

[21] *See* 17 CFR § 229.303.

[22] *See, e.g.,* 17 CFR § 229.105.

obtain through existing corporate disclosures combined with shareholder engagement programs, proxy advisor reports, and corporate governance ratings.

A. New Expertise Disclosures May Lead to "Special Interest" Directors.

While public companies already provide details about the business experience and expertise of their board members, the proposed rule would mandate additional disclosure about whether they have a director with expertise in cybersecurity, with very specific guidance about what might constitute this expertise. For instance, the proposed rule gives as examples prior experience as a chief information security officer ("CISO") or a security policy analyst or having a degree in cybersecurity. While the SEC also allows for "knowledge, skills, or other background in cybersecurity, including, for example, in the areas of security policy and governance, risk management, security assessment," the examples in this section indicate a preference for those who have been primarily employed in cybersecurity roles.

We believe this specific expertise disclosure mandate will decrease, rather than increase, the effectiveness of board oversight of cybersecurity, as well as its oversight of other issues. While it is important for boards to have a mix of directors with different skills and qualifications, those skills are generally considered broadly – companies often disclose that their directors have experience with areas like "marketing" or "international business," for instance, rather than trying to closely tie such skills to the specific roles, work experiences, and educational background. We believe this is appropriate for the role that directors play – a board of directors should not operate as a second management team, with individual directors replicating the most important management roles.[23] Rather, a board exists to provide high-level oversight of strategy and operations, helping ensure management is balancing priorities, taking advantage of opportunities, and protecting against risks.

This prescriptive approach to director expertise is not necessary given the director business experience disclosures now provided by companies. Even for those directors who fill the important role of audit committee financial experts, that expertise involves only an "understanding" and an "ability to assess" the relevant issues. This understanding and ability do not require the director to have worked directly in finance and can be obtained by having been in

[23] "While each board member is responsible for acting with due care and loyalty and informing himself or herself about and approving major corporate action, directors are not active managers. Rather, the board's functions are generally limited to (1) authorizing major corporate actions, (2) advising corporate management, (3) assuring the efficacy of corporate reporting and auditing procedures in order to remain adequately informed of the corporation's financial status, (4) regularly reviewing the corporation's investments to insure compliance with all applicable provisions of law, and (5) monitoring the performance of management, setting goals, and measuring management's results against them." § 1:2. Responsibilities of directors and officers, Law of Corp. Offs. & Dirs.: Rights, Duties & Liabilities § 1:2 (2021-2022).

a position of *actively supervising* others who do so.[24] In some instances, for example, experience as a CEO can qualify a director as an audit committee financial expert. Nasdaq Listing Rule IM-5605-3(2)(A) explicitly lists CEOs among those who have "financial sophistication" for the purposes of its related listing requirement. Similarly, valuable cybersecurity expertise can be gained through service as a CEO, COO, or other supervisory officer of a company with a robust cybersecurity program; through managing other companies that experienced cyber incidents; or through many other paths that do not necessarily satisfy the proposed rule's narrow definition.

We have also noted that the SEC has taken a similar approach to disclosure of the presence of climate change expertise in its proposed disclosure rules about that topic, demonstrating that this may be part of a new trend in SEC rulemaking.[25] We are concerned that the SEC's new approach will put pressure on issuers to place directors on their boards who possess narrow technical skills reflecting the Commission's latest priorities, with overall negative effects on board governance.

In 2018, when the U.S. Senate was considering the Cybersecurity Disclosure Act, which would have legislatively required issuers to disclose whether their boards contained cybersecurity experts, our CEO, Darla Stuckey, testified to the Banking Committee about the risks of appointing "special interest" directors to boards.[26] During her testimony, she quoted a Society member:

> *Of course, we want our public companies' boards to have the requisite skills to deal with all sorts of issues. However, specifying the types of skills that a company's board must have strikes me as the ultimate one-size-fits-all approach and has no logical limits. Should every public company have an expert on revenue recognition? Related-party transactions? Has anyone thought through the consequences of having a board comprised of one-issue experts who may not have any other applicable skill sets? And would a cyber-expert want to be on a board, given that he or she would likely be blamed (and possibly sued) if the company had a breach or other cyber problem?*

[24] Reg. S-K, § 407(d)(5)(ii) & (iii).

[25] Release Nos. 33-11042; 34-99478.

[26] *Legislative Proposals to Examine Corporate Governance: Before the Senate Committee on Banking, Housing and Urban Affairs* (Statement of Darla C. Stuckey, President & CEO, Society for Corporate Governance), https://www.banking.senate.gov/imo/media/doc/Stuckey%20Testimony%206-28-18.pdf, at page 17. Following this testimony, and other testimony and debate, the legislation did not pass.

We reiterate the concerns Ms. Stuckey raised in her 2018 testimony. We are concerned that, especially given the well-known shortage of cybersecurity professionals,[27] and the potential that candidates may be concerned about personal liability for incidents if they join a board, it will be extremely difficult for issuers to find directors who meet the criteria the SEC has laid out for cybersecurity expertise who also have the broader skills and experiences needed to perform the rest of their board oversight responsibilities – including oversight of business strategy, legal and regulatory risk management, budgeting, financial reporting, executive compensation, and human capital management.

The need for specific areas of expertise/skills on the board also varies by company and industry. Many issuers already voluntarily disclose the cybersecurity experience of some of their directors, with that expertise varying in nature and depth depending on the company and the industry. Very frequently, directors are not needed to act as technical cybersecurity experts, as management has that expertise. When a board determines there is a need for additional expertise, it can ask management to provide briefings from third parties or retain them directly.[28]

As Ms. Stuckey also testified in 2018, directors do not typically receive the detailed operational information needed to act as second CISOs, even if that were appropriate roles for them. We are concerned that companies that add technical cybersecurity expert directors to their boards may, in some cases, give investors a false sense that the board is more actively involved in managing company cybersecurity risk than it could possibly be. Indeed, if the presence of a designated cybersecurity expert on a board causes the other directors to defer to that expert on matters related to cybersecurity, rather than engaging in a full deliberative process, the presence of the expert could even diminish the quality of cybersecurity oversight.

If investors do not believe that the composition of a particular board is adequate to address cybersecurity risks at any particular issuer, they can ask the issuer for more information about the expertise of existing directors and any external advisors. The proposed rule's "one size fits all" approach is, we believe, unnecessary and potentially harmful.

---

[27] "Organizations such as the International Information System Security Certification Consortium, or ISC2, say the demand for cybersecurity workers is far outstripping the available workforce," and "around 2.72 million more cybersecurity workers are needed globally." James Rundle and Kim S. Nash, "Cybersecurity: Cyber Chief Try New Tactics to Get Talent," WALL ST. JOURNAL, April 21, 2022, at B5.

[28] In a recent interview with PJT Camberview's email newsletter, John Galloway, global head of investment stewardship at Vanguard, expressed a similar view about cybersecurity expertise: "On a topic like cybersecurity, we do not believe that every board needs a cyber expert per se. But we would expect boards to ensure they have access to the appropriate external expertise so that they can develop an understanding of the topic and provide appropriate, independent oversight. This is an area where we are actively engaging with companies and asking them to disclose how their board is addressing any gaps in skills or expertise related to cyber (as we do with other material risks)." *See* PJT Camberview, "Engaging with Vanguard," May 9, 2022.

If the Commission concludes that more detailed disclosure about the cybersecurity expertise of the board is warranted, a less prescriptive approach would be simply to ask each issuer to explain why it believes the board, collectively, has the ability to oversee these risks adequately. This disclosure, which could appear in the proxy statement where governance matters typically reside, should satisfy the Commission's concerns without raising as many of the risks identified above.

Finally, we also note that the proposed rule contemplates that disclosure about director expertise be presented in an Interactive Data File (*see* proposed Reg. S-T, § 232.405). Proxy statements are not ordinarily presented in that manner, and we would encourage the SEC to eliminate that technical requirement.

B. Board and Committee Process Disclosures Are Unnecessary and Potentially Deleterious.

The degree of disclosure the proposed rule seeks about board and committee processes is unprecedented and may actually decrease the quality of governance and board oversight. We have no objection to the requirement that companies clearly disclose where governance of cybersecurity sits – on a particular committee or the full board. That is not an unusual requirement, as companies are already required to disclose, generally, how their boards manage risk.[29]

The proposed rule goes far beyond that, however, requiring disclosure of "the processes by which the board is informed about cybersecurity risks, and the frequency of its discussions on the topic" and "whether and how the board or board committee considers cybersecurity risks as part of its business strategy, risk management, and financial oversight." Again, we note that the Commission is seeking similar information in its proposed rule about climate risk disclosure. We are concerned that the SEC may be embarking on a wholesale expansion of disclosure about governance, which may lead companies to regularly disclose significant portions of their board and committee calendars, agendas, and materials. This would significantly change the way boards operate with unknown, and we believe, deleterious, effect.

The Society believes that requiring disclosure of the frequency of board or committee discussion of cybersecurity risks would elevate form over substance. Required disclosure of discussion frequency will inevitably put pressure on issuers to make cybersecurity a more frequent agenda topic. But frequency is only part of the story of governance – the quality of oversight depends on many other factors, such as candor and the nature of the information provided to directors. The appropriate frequency of such oversight also varies from one company

[29] *See* Reg. S-K, § 407-h.

to another for many reasons, some of which are obvious to investors (the nature of the business) but some of which are not (management expertise and the quality of informal discussions between directors and management between meetings). Disclosing frequency can also reveal confidential information that could provide unintended assistance to malicious actors or competitors – for instance, if a company had a confidential need to meet more regularly on cybersecurity risks in a particular year.

With respect to the processes by which the board is informed about cybersecurity risks, it is unclear what sort of disclosure SEC is looking for. Should companies disclose the number of pages of materials that directors review or the names of the in-house and external experts they speak with? It is particularly hard to anticipate what the SEC is seeking with this proposed requirement, because no other SEC rule seeks such detailed board process information, a fact which should itself raise questions about its appropriateness.

The proposed usefulness to investors is even less clear. If issuers decide that their investors would benefit from hearing more detail about their board review process for cybersecurity, they are free to provide that information. Investors are also free to ask for it. The rationale for requiring this kind of disclosure at *every* company, however, is lacking. As a practical matter, this disclosure is going to be so general as to be useless or it is going to risk revealing confidential information about a particular company that could be improperly used by malicious actors or competitors.

This problem is exacerbated by the proposed rule's detailed requirement that an issuer also discloses how the board specifically considers cybersecurity as part of company strategy, risk management, and financial oversight. What the SEC imagines this disclosure would contain is similarly unclear, particularly (again) because there are no existing disclosure requirements that take this form. Company strategy choices made by a board, and the reasoning behind them, are not ordinarily disclosed in SEC filings, and for good reason. Many issuers will find it difficult to say anything meaningful about these specific topics that avoids disclosure of confidential information that may be sensitive. Rather than turning to the boilerplate disclosure likely to be inspired by the proposed rule, investors who have concerns about a particular board's decision-making would be better served by engaging with the issuer or using the mechanisms provided by state corporations law to gain more information.

C. New Management Disclosures Would Not Be Helpful to Investors.

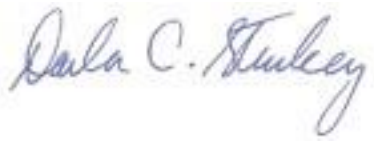
We believe that similar concerns arise from the proposed disclosures about the management of cybersecurity risks, another sort of disclosure requirement without real precedent. Existing rules around MD&A disclosure should be sufficient to elicit relevant information, and if needed could be supplemented to include discussion of the company's

approach to cybersecurity risk management and strategy. If issuers are compelled to disclose who on their management team is an expert in cybersecurity, where that expertise comes from, where they fit in the organization, and how often they meet with other management experts and the board, the temptation will be to create a program that an issuer believes will look good to investors – and one that looks like other issuers' programs – regardless of that company's particular needs. These detailed requirements may also disincentivize issuers from changing their personnel or programs, even where change would improve the management of cybersecurity risk. It also appears disproportionate to any conceivable investor interest – why should an investor need to know more about a company's CISO than it does about its CEO? In addition, disclosing a company's policies and procedures provides a potential road map to potential vulnerabilities in the oversight of its information systems. This proposed mandate is without precedent in existing securities disclosure requirements, and we are concerned that the SEC has not fully considered the implications of this more intrusive and prescriptive approach.

Thank you for considering the Society's views on cybersecurity disclosure.

Respectfully submitted,

Ted Allen
Vice President, Policy & Advocacy
Society for Corporate Governance



Darla Stuckey
President and CEO
Society for Corporate Governance