American Property Casualty Insurance Association
INSURING AMERICA apci.org

May 9, 2022

Vanessa Countryman, Secretary
Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-0609
Via www.sec.gov/cgi-bin/ruling-comments

Re: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure
File Number: S7-09-22

Dear Ms. Countryman:

The American Property Casualty Insurance Association (APCIA) appreciates the opportunity to comment on the Securities and Exchange Commission's proposed rules regarding cybersecurity risk management, strategy, governance, and cybersecurity incident reporting by public companies. APCIA is the primary national trade association for home, auto, and business insurers. APCIA promotes and protects the viability of private competition for the benefit of consumers and insurers, with a legacy dating back 150 years. APCIA members represent all sizes, structures, and regions—protecting families, communities, and businesses in the U.S. and across the globe.

Property casualty insurers are working to increase the nation's cyber resilience by encouraging greater cybersecurity, preparedness, and threat information sharing with government officials to thwart cyber-attacks. Many APCIA members provide cyber insurance products to their customers. Cyber insurance is a beneficial tool to create awareness of the risk and encourage adoption of robust security measures to support our nation's cyber resilience. As cyber threats have grown, so too has the role of insurers. For example, insurers are increasingly stipulating that organizations adopt security controls that can make a measurable, positive impact on their exposure to cyber risk.

APCIA is concerned that the proposed rules will create significant new risks for insurers and their policyholders. In addition, the proposed rules go beyond what is necessary to meet the objectives of protecting investors and providing a better understanding of registrants' cybersecurity risk – seemingly expanding the SEC's role into the realm of cybersecurity regulation. We encourage the SEC to reevaluate whether its approach to cybersecurity disclosures is necessary in light of the plethora of state and federal cybersecurity laws, including the recently enacted Strengthening American Cybersecurity Act. In the event the SEC determines to move forward with establishing cybersecurity regulations, the focus should be on creating a structure for harmonizing the array of existing cybersecurity reporting standards, rather than establishing a competing and conflicting standard. We offer the following comments on the proposed rules if the SEC nonetheless moves forward with this proposal.

Incident Reporting

We encourage the SEC to reconsider the timing for disclosing a material cybersecurity incident and to permit a filing delay under certain enumerated circumstances.

Under the proposed rules, registrants must disclose a material incident within four business days after the registrant determines that a cybersecurity incident it has experienced is material, even if the vulnerability remains active, no patch or fix has been made available, law enforcement has requested a delay, or an investigation remains ongoing. As described in more detail below, this requirement complicates a registrant's ability to respond in a controlled manner, frustrates law enforcement efforts, may increase the severity of an incident, and could be exploited by bad actors, including to attack other companies that may be unaware of the vulnerability in question.

To alleviate some of these concerns, we recommend the SEC provide an option to a registrant to delay reporting for up to 30 days (as opposed to four days) after the materiality determination under the following circumstances: (1) where a registrant reasonably believes that disclosure of the cybersecurity incident would materially disadvantage the registrant's ability to contain and remediate the incident, or (2) at the request of law enforcement.

If filed after four days, the Form 8-K disclosure could be required to include a discussion of the registrant's rationale for the filing delay. We believe that permitting a registrant to delay the filing for a short period of time strikes an appropriate balance between timely disclosure to shareholders and an opportunity for a registrant to achieve the best resolution for itself and its shareholders. Allowing up to 30 days for disclosure would also bring the SEC's proposal in line with data breach disclosure requirements at the state level.

The SEC should allow an extension of cybersecurity incident disclosures because companies need flexibility to employ a variety of methods and strategies to respond to and remediate an incident. In some instances, registrants may need to monitor a situation before reporting in order to best contain and mitigate the incident. In others, law enforcement may recommend a course of action that could extend beyond four days, or the incident may stem from a third-party vendor and a registrant may be dependent on the third party to conduct an appropriate investigation and to provide relevant information.

For example, if a registrant were to find malware or ransomware on its system that had not yet been triggered, the best approach may be to watch the activity on the system (for more than four days) to identify an approach to contain the malware/ransomware before it spreads. Disclosing the event would alert the bad actor about what the registrant knows which may accelerate the bad actor's efforts to the registrant's detriment. Likewise, delaying public disclosure may also be necessary in a situation where a zero-day incident is discovered or where an incident is not yet widely known but is believed to have a potentially significant impact (e.g., SolarWinds and Log4j). In these instances, reporting the incident publicly before a patch has been issued would put the registrant and other companies defending against the attack at a disadvantage compared with malicious actors seeking to exploit the vulnerability.

Public disclosure of real or perceived system vulnerabilities prior to remediation may also put other bad actors on notice and provide an opportunity for vulnerabilities to be exploited. Moreover, premature public disclosure would lead to numerous inquiries from outside parties, such as regulators, shareholders, and the media. An unintended consequence of premature disclosure is that registrants may have to divert much needed attention and resources away from the incident response to handling those inquires. Investors would also receive incomplete information that will likely change as the incident investigation progresses. Instead, the SEC should allow sufficient time to remediate a cyber incident prior to any mandated public disclosure.

Safe Harbors
APCIA supports the SEC's inclusion of safe harbors for failing to timely file a Form 8-K disclosure, and we would expect the safe harbor to extend to any reporting delay. (See Proposed Rules §§ 13a-11(c) and 15d-11(c)). The safe harbor appropriately recognizes the fluid nature of cybersecurity incidents, materiality assessments, and corrective efforts.

Third-Party Breaches
APCIA recommends clarifying the proposed definition of "information systems," which the rule currently defines as "information resources owned or *used by* the registrant…." (Emphasis added.) The language "used by" would require that a registrant disclose a cybersecurity incident of a third-party provider, which could include, for example, an incident impacting a shared data center. However, registrants using third-party providers may not receive timely notice of the incident and may not receive the information that a registrant is required to provide in its Form 8-K. Worse, requiring disclosure of vendors in the event of a data breach could expose a registrant to new threats from malicious actors seeking access points to the registrant's systems. To address these concerns, the definition of "information systems" should be limited to systems managed by a registrant or systems managed at a registrant's direction.

Alternatively, we encourage the SEC to clarify that a registrant's filing requirement for a cybersecurity incident involving a third-party provider is not triggered until the registrant has received actual notice of the incident and has made the materiality assessment. Even with this clarification, a registrant would be required to make reasonable inquiries of the third-party provider to obtain the information needed for the required disclosure. We further recommend that the safe harbor described in the proposed rules (§§13a-11(c) and 15d-11(c)) be extended to include, in addition to failing to timely file, deficiencies in the disclosure to the extent the missing information was not available from the third party.

Threats
APCIA is concerned that the examples of cybersecurity incidents that may be subject to disclosure include circumstances where "a malicious actor has offered to sell or has threatened to publicly disclose sensitive company data". This could potentially require disclosure simply because someone makes a threat, even if the bad actor does not actually have access to a registrant's data. Such disclosures are unnecessary and would be potentially misleading or confusing for investors. In addition, we are concerned this requirement could lead to a whole new class of attack, where a bad actor could attempt to extort a company by demanding payment in exchange for the bad actor not making a threat that would trigger a public disclosure.

To address these concerns, this example should clarify that threats do not need to be disclosed unless there is cause to believe a malicious actor actually possesses or has access to sensitive company data. Previous guidance from the SEC already establishes criteria that should be used by companies to determine the materiality of an incident. However, this example and others seem to lower the existing threshold and introduce more uncertainty.

Series of Incidents
We are also concerned with the proposed requirement for companies to disclose, to the extent known to management, when a series of previously undisclosed individually immaterial cybersecurity incidents has become material in the aggregate. This would potentially require companies to go back several years or an indefinite period to determine whether cybersecurity incidents are material. Materiality may change with additional investigation, and the point at which the four-business-day reporting requirement begins is unclear. It is also unclear what creates a series of incidents—multiple attacks from the same attacker, multiple attacks originating from the same country, multiple attacks of the same type from different attackers, etc.

To create a more workable standard, the proposal should set a one-year limitation to the analysis of when a series of previously undisclosed individually immaterial cybersecurity incidents has become material in the aggregate. The proposal should also specify what constitutes a series of incidents. Registrants should not be required to consider individually immaterial incidents unless the incident took place within the last year and the incidents are clearly connected. A longer lookback period would be overly burdensome for companies, with limited or no benefit to investors.

Risk Management, Strategy, and Governance

Risk Management and Strategy
APCIA strongly urges the SEC to reconsider the proposed rules' requirement for registrants to disclose their cybersecurity risk oversight, strategy, policies, and procedures. These disclosures would provide a blueprint of a company's vulnerabilities to malicious actors, causing significant new threats to both insurers and their policyholders. Moreover, insurers are already subject to substantial cybersecurity governance and compliance requirements at both the state and federal levels.

In response to escalating cyber risks and increasing regulation, insurers and their policyholders have adopted robust security controls, and insurers continue to invest in new technologies designed to help public and private sector policyholders minimize and protect against cyber threats. Requiring disclosure of these strategies would neutralize their effectiveness and potentially harm the nation's cyber resilience. It could even lead to potentially more cyber-attacks to the extent companies are required to disclose details that would relate to their cyber insurance coverage. Further, it is unclear how investors would benefit from these disclosures. In any event, the inherent risk involved with disclosing a company's cybersecurity strategy far outweighs any benefit the disclosures would provide.

Board of Directors' Cybersecurity Expertise
Finally, the SEC should reconsider mandating disclosures about the cybersecurity expertise of members of a company's board of directors. If enacted, these disclosure requirements would likely transform into a *de facto* requirement for registrants to find board members with cybersecurity expertise because the absence of such board expertise may be misconstrued by the public as a signal that a company does not take cybersecurity seriously. Perceived gaps in cybersecurity expertise on the board could also lead to a proliferation of securities litigation, including for companies that, in fact, have robust cybersecurity controls. However, no evidence has been provided by the SEC that this would improve the cybersecurity posture of registrants or provide additional benefits to investors.

Since companies commonly maintain vigorous cybersecurity programs without specific board expertise, these proposed disclosures would provide little, if any, benefit toward furthering the proposal's objective of giving investors a better understanding of registrants' cybersecurity risk. In fact, the proposal could create new cyber vulnerabilities by exacerbating demand for cybersecurity professionals. By encouraging companies to hire cybersecurity experts to board positions, the field of potential qualified candidates to fill these positions – which is already scarce – would shrink even further. According to the tracking site Cyber Seek (www.cyberseek.org), in the U.S. there are currently 597,767 cyber-security positions open within 1,053,468 total jobs, or 56.7% of all positions need to be filled. Additionally, per Cyber Seek, there are only enough cybersecurity workers in the United States to fill 68% of the cybersecurity jobs that employers demand. APCIA is concerned that the knock-on effects of this proposal will make it more difficult for insurers and their policyholders to find the talent necessary to stem the increasing and ever-evolving threat of cyber-attacks.

Thank you again for the opportunity to provide feedback, and we welcome additional dialogue should you have any questions.

Sincerely,

Matthew Vece
Director, Financial & Tax Counsel
[redacted]

Gary P. Sullivan, CPCU, AIC, AIM, AIS
Sr. Director, Emerging Risks
[redacted]