Via SEC.gov

May 9, 2022

Vanessa A. Countryman, Secretary
Securities and Exchange Commission
100 F Street, NE
Washington, D.C. 20549


Dear Ms. Countryman:

Consumer Technology Association (CTA) \(^1\) respectfully responds to the Securities and Exchange Commission’s (SEC’s) Proposed Rules for Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure (Proposed Rules). \(^2\) Cybersecurity is top of mind for CTA members and CTA has worked closely with government partners to promote innovative solutions to meet the challenging demands of the ever-evolving threat landscape. CTA members know that cybersecurity risk management requires accountability and communication across organizations—from decisionmakers to product designers—and collaboration with partners both public and private.

CTA appreciates the SEC’s interest in ensuring investors are meaningfully informed about cybersecurity events and practices through appropriate disclosure rules, but we are concerned that the Proposed Rules, as drafted, may in some cases adversely affect the security posture of publicly traded companies as well as the broader cybersecurity ecosystem, and hamper ongoing operational cyber incident response efforts. Specifically, the SEC should take additional steps to develop the record to ensure the agency does not adopt rules that would undermine cybersecurity through public disclosure of unmitigated vulnerabilities and threats, are inconsistent with international best practices and conflict with related efforts at other agencies.

\(^{1}\) As North America’s largest technology trade association, CTA\(^\circledast\) is the tech sector. Our members are the world’s leading innovators—from startups to global brands—helping support more than 18 million American jobs. CTA owns and produces CES\(^\circledast\)—the most influential tech event on the planet.

Build a Robust Public Record to Inform Revised Proposed Rules.

CTA recognizes the SEC’s interest in ensuring shareholders have access to information regarding cybersecurity events and practices that can inform or undermine their investments in public companies. Indeed, the SEC has included cybersecurity within its disclosures regarding material risk for many years. However, the Proposed Rules purport to expand the nature and scope of these mandatory disclosures in ways that may undermine the cybersecurity practices and goals of public companies and infringe on the efforts of other agencies with operational cybersecurity missions—absent a well-developed record to support these changes. The specific disclosures, such as the four-day rule, would in some cases require public companies to prematurely disclose vulnerabilities principally for the sake of regulatory compliance rather than for a cybersecurity purpose. The premature public disclosure of a vulnerability before remediation, could have disastrous cybersecurity effects for the disclosing company as well as numerous other organizations, depending on the nature of the vulnerability.

Given the complicated set of challenges involved in cybersecurity disclosure, the SEC should take additional steps to solicit input and develop a more robust record prior to releasing revised proposed rules. Indeed, cybersecurity is exactly the type of complicated issue the SEC has indicated deserves public input—such as a public notice or hearing with informed testimony and evidence from cybersecurity professionals, as well as government agencies specifically charged with developing and implementing cybersecurity policy and ensuring security in the nation’s digital ecosystem including the Cybersecurity and Infrastructure Security Agency (CISA) and the Office of the National Cyber Director—prior to issuing a detailed proposed rule. This is an especially important step because other federal agencies are developing cybersecurity management, reporting and other best practices that the Proposed Rules may contradict.

Although the SEC held a roundtable that included some discussion of aspects of cybersecurity disclosure in 2014, the cybersecurity landscape has evolved significantly over the last eight years and federal reporting frameworks have evolved along with it. Coming at this time, the SEC’s disclosure requirement could be seen as prematurely wedging itself into established and evolving cybersecurity practices still in development throughout industry and the government, as discussed in the next section. To avoid such conflicts, CTA urges the SEC to solicit input from the widespread diaspora of stakeholders engaged on these issues outside the present notice.

---

3 As 2011 SEC disclosure guidance notes, "material information regarding cybersecurity risks and cyber incidents is required to be disclosed when necessary in order to make other required disclosures . . . as with other operational and financial risks, registrants should review, on an ongoing basis, the adequacy of their disclosure relating to cybersecurity risks and cyber incidents." See Securities and Exchange Commission, Division of Corporation Finance, CF Disclosure Guidance: Topic No. 2 – Cybersecurity (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.
4 SEC, Rulemaking Process, Audit No. 347, (Jul. 12, 2002), available at https://www.sec.gov/oig/reportspubs/aboutoigaudit347finhtm.html (noting that “if an issue is unique or complicated, the Commission may first seek out public input on which, if any, regulatory approach is appropriate,” which may be conducted in the form of a concept release, roundtable discussions, or hearings).
and refine the Proposed Rules to more narrowly target the types and timing of disclosures needed to achieve the SEC’s goals, while ensuring that such rules would not undermine efforts to remediate and recover from cybersecurity incidents and threats. This process should include additional engagement with critical infrastructure sectors and the SEC should provide a revised set of Proposed Rules for public comment.

**Cyber-Related Disclosure Should be Complementary to Industry Best Practices.**

Any SEC rule should complement—not contradict—established industry practices that support ongoing innovative cybersecurity risk management. Companies across the globe have collaboratively developed common approaches to identifying, managing and communicating risk, such as through use of the National Institute of Standards and Technology’s (NIST’s) *Framework for Improving Critical Infrastructure Cybersecurity*. Tools like these help public companies continually enhance their cybersecurity postures, respond to and recover from cyber incidents when they occur, through mechanisms that can be translated, tailored and adapted to meet evolving needs. In addition, industry itself has developed common practices to perform specific tasks through standards, such as the ETSI coordinated vulnerability disclosure (CVD) process.

CTA acknowledges that there are situations where cybersecurity reporting requirements designed to protect our national critical infrastructure play an important role, especially if narrowly tailored to achieve their public policy aim. However, the Proposed Rules would require public companies to report a material cyber incident within four business days of a company determining such an incident has occurred, yet do not provide an exemption to this four-day requirement to account for the needs of organizations working to remediate the threat, law enforcement or national security activities, nor do they account for companies working through CVD processes. Furthermore, the Proposed Rules would require reporting entities to disclose whether they have completed mitigation of the vulnerability in question, further risking exploitation of the vulnerability by bad actors. Timing needs can vary and critically impact CVD processes, which enable entities to collaboratively address security flaws without aiding malicious actors in additional exploitation of a vulnerability. Moreover, this four-day requirement may conflict with reporting requirements at other agencies focused on operational cybersecurity, such as CISA’s forthcoming rules on cyber incident reporting for

---


9 Proposed Rules at 16607.

10 Grossman-Bergman Blog.
critical infrastructure. For these reasons, establishing a required timeline for disclosure would distract from, interfere with or could otherwise lead to incomplete information about an ongoing cyber incident.

The proposed rule’s incident-reporting obligations may also negatively impact critical cybersecurity information-sharing practices, to the detriment of companies, their investors and the public. Following Presidential Decision Directive/NSC-63, many critical industries have established Information Sharing and Analysis Centers (ISACs). Information shared with industry and government is designed to help all promptly identify and mitigate significant security risks as identified by member companies. The proposed rule may have an unintended chilling effect on this information sharing. If subject to the Proposed Rules, ISAC members may now hesitate to characterize risks with the appropriate degree of severity, or share them at all, if their decision to share and characterize a risk as critical is later challenged if the company did not disclose a related incident as material. Particularly given the sophisticated, evolving threats faced by the U.S. government and the private sector partners on which it relies, agencies across the federal government should find ways to incentivize—not hinder—cyber threat information sharing.

In addition, any rules regarding cybersecurity disclosure should not artificially distort the board appointment decisions of public companies in ways that may not provide meaningful information to shareholders. For example, the Proposed Rules would require companies to disclose whether any members of its board of directors have cybersecurity expertise and describe the nature of that expertise. While CTA agrees that cybersecurity already is and should always be among the top priorities for most public companies, “cybersecurity expertise” by its nature is diverse—it can be both sector-specific and dependent on the innovative capabilities of interdisciplinary experts—and likely cannot be adequately quantified in an SEC disclosure. Such a requirement would more likely push companies to “check the box” with token qualifications among one or more board members, rather than a discerning, holistic suite of risk management experience and expertise—including diverse cybersecurity experience and expertise—that companies apply in their board appointments.

Any Rules Must Contribute to a Coordinated, Dynamic, Adaptive Cybersecurity Approach.

To effectively address the cybersecurity challenges facing our nation, the Biden Administration and independent federal agencies are working to coordinate a dynamic, whole-of-government approach. The National Security Council is leading coordination of this effort given its visibility across relevant agencies, and Congress has specifically directed CISA to lead development of

---

13 Proposed Rules at 44.
cyber incident reporting rules.\textsuperscript{14} Any rules the SEC adopts should complement those efforts and the SEC should be careful not to act in a silo on these issues. Nor should it presume a one-size-fits-all-sectors approach.

Any required disclosure should avoid reliance on a calcified compliance checklist that commits companies to practices that become rapidly outdated as the threat landscape evolves. Likewise, care should be taken such that a company is not required by law to disclose information that would unintentionally benefit malicious actors, such as details regarding specific practices or response playbooks.

Should the SEC develop final rules in this proceeding, it should do so with an understanding that different sectors have different needs and each actor in the ecosystem—public or private—must bring its unique expertise and tools to bear to support an operational and collaborative approach to cybersecurity. The SEC should further this process by tailoring its focus to its mission and supporting a proactively harmonized whole-of-government process—strategically aimed at achieving the government’s goals.

CTA appreciates the opportunity to provide the input above and welcomes continued engagement on this critical issue.

Respectfully submitted,

\textit{/s/J. David Grossman} \\
J. David Grossman \\
Vice President, Regulatory Affairs

\textit{/s/Mike Bergman} \\
Mike Bergman \\
Vice President, Technology & Standards

\textsuperscript{14} See generally, CIRCIA.