June 22, 2022

Vanessa A. Countryman
Secretary
Securities and Exchange Commission
Washington, DC 20549

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

Dear Ms. Countryman:

Our organizations, which represent sectors across the U.S. economy, write to provide input on the Securities and Exchange Commission's proposed rules on *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*.

Collectively, our associations appreciate the goals of the SEC's proposed rules, which focus on increasing investors' knowledge of publicly traded companies' cybersecurity postures. We agree with Chair Gensler's view that "[a] lot of issuers already provide cybersecurity disclosure to investors" and that "companies and investors alike would benefit if this information were required in a consistent, comparable, and decision-useful manner."

However, the SEC's proposed reporting regime departs significantly from the Commission's 2018 interpretive guidance, which effectively balances investor interests with companies' cybersecurity disclosure obligations. The proposed rules could result in undermining cybersecurity by forcing companies to disclose incident information prior to the mitigation of vulnerabilities. Detailed public disclosures could give cybercriminals and state-backed hackers a trove of data to further victimize companies, harm law enforcement investigations, and disrupt public-private responses to cyberattacks. Also, the costs of the rulemaking outweigh its benefits to investors. Simply put, the proposed rules go too far and would place companies at heightened risk by compelling them to prematurely disclose increased amounts of cybersecurity incident information.

Many in the business community strongly believe that the Commission's proposal should not be finalized in its current form. Calibrating the rulemaking correctly requires the SEC to proceed with caution and coordinate with other parts of the federal government. Given the complexity of the proposal, as well as its impact on U.S. economic security and cybersecurity, the Commission should allow more time for industry input.

While this list is not exhaustive of our groups' views, we urge the Commission to consider the following points as it seeks to develop a cybersecurity incident and risk management disclosure regime that both informs investors and protects companies against malicious actors.

- **The disclosure of cybersecurity incidents should accommodate temporary delays for law enforcement and/or ongoing investigations.** The Commission's proposed rules need to be revised so that companies can temporarily delay reporting on material cybersecurity incidents because of law enforcement and/or ongoing national security investigations against illicit hackers where U.S. cybersecurity is at stake. Instead of undercutting industry-government cooperation, the SEC should urge companies to work with law enforcement and national security agencies to mitigate the impacts of cyber incidents and help bolster companies' security and financial positions, which would benefit investors.

  More specifically, all 50 U.S. states have passed laws authorizing delayed disclosures to consumers of breaches of their sensitive personal data to avoid compromising an ongoing law enforcement investigation. The Gramm-Leach-Bliley Act similarly authorizes such delayed disclosure by financial institutions, and federal law enforcement agencies make such requests of registrants in appropriate circumstances. Without a corresponding law enforcement exception, the proposed rules would undermine the judgment of the states and several federal agencies that law enforcement protects the public first.

  The Commission's proposed rules should enable companies to delay disclosures due to active investigations by law enforcement and other reasonable requests (e.g., to remediate a cybersecurity incident) like other state and federal reporting laws. Companies need time to conduct internal investigations to accurately determine an incident's true scope and impact. The proposed rules could easily compel companies to make premature disclosures driven more by compliance timelines than genuine cybersecurity incident remediation factors. Companies are rightly concerned that SEC requirements mandating them to report incident and vulnerability information too early could place them at greater risk.

  Further, hasty reporting may not necessarily be accurate, given the little time afforded to companies to report material cybersecurity incidents. It is possible that the severity of incidents could be overstated, thus having a potentially negative effect on a company's earnings.

- **The rulemaking should not override laws and regulations related to cybersecurity and protected disclosures.** The Commission's proposal overwhelmingly conflicts with the policy goals established by Congress in recent cybersecurity legislation, especially the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), which was signed into law on March 15—less than a week after the SEC announced its cybersecurity proposal. The new law requires certain critical infrastructure entities to report on a confidential and protected basis covered cyber incidents to the Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours. Congress intended CISA to be the primary entity for reporting cybersecurity incidents to the federal government. Lawmakers also said that a business should only have to report to federal agencies once.

Congress has explicitly emphasized the importance of protecting cybersecurity incident data from unwarranted disclosures. For companies that perform work for the Department of Defense (DoD), the SEC's proposed rules neither recognize nor align with the evolving cybersecurity standards and disclosures required of these contractors. Several years ago, DoD initiated a Cybersecurity Maturity Model Certification (CMMC) program for contractors that seeks to leverage existing standards associated with the National Institute of Standards and Technology (NIST) Special Publication 800-171 to protect controlled unclassified information in nonfederal systems and organizations. The SEC does not appear to consider the potentially contradictory, unnecessarily duplicative, or financially burdensome nature of its proposed rules when compared with the CMMC requirements.

Requirements under the CMMC process are evolving as DoD continues to adjudicate industry comments regarding its September 2020 interim rule, while working to publish another interim rule in early 2023. The CMMC process holds companies to a higher standard of cybersecurity than what is required of government agencies. The Commission appears to do the same with its proposed rules, which contributes to an imbalance of public- and private-sector responsibilities.*

Congress also clarified that vulnerability information should be coordinated based on principles consistent with international standards and leading industry practices requiring protection and strict confidence.

- **The practicality and value of disclosing "aggregate" cybersecurity incidents are unclear.** The proposed rules would require a company to disclose when a series of previously undisclosed cybersecurity incidents become material in the aggregate. The Commission's proposal is notably vague about when a number of individual cybersecurity incidents—taken together—would be considered materially reportable. Only in hindsight and with considerable business and government effort can some hacking campaigns be grouped together. The Commission does not seem to consider the costs and the difficulty of identifying and tracking material incidents in the aggregate. The feasibility and value of aggregate reporting to investors is questionable.

- **The unprecedented micromanagement of companies' cybersecurity programs is misguided and would not necessarily protect investors.** The proposed rules embody an unnecessary micromanagement pertaining to the composition and functioning of both the management and the boards of companies. The SEC should not insert itself via disclosure rules into how a company would design its plans to detect, respond to, and recover from cyber incidents. The proposed rules could put companies in jeopardy by forcing them to allocate resources toward compliance-based reporting rather than triaging the complex elements of identifying and resolving cybersecurity incidents. If shared prematurely, the

* Additional federal laws and regulations that mandate the protection of cybersecurity-related information include the Chemical Facilities Anti-Terrorism Standards program, the Critical Infrastructure Protection Reliability Standards program, the Health Insurance Portability and Accountability Act of 1996, and the Maritime Transportation Security Act of 2002.

public disclosure of vulnerability data could give attackers a roadmap to exploit reporting registrants.

Similarly, disclosing the finer points of a company's cybersecurity policies and processes is excessive. This requirement would make the registrant an attractive target for malicious actors that could acquire unwarranted insights into a company's practices and develop a game plan for future exploitation. A cybersecurity program reflects a company's tailoring of the relevant laws, regulations, and standards that fit its unique structure and business environment. The proposed governance disclosures, moreover, take a detailed, one-size-fits-all approach, which implies "best practices" that would not make operational sense to each company.

- **Agencies, including the SEC, need to prioritize streamlining reporting regulations.** The SEC's proposed rules leave businesses in the unfavorable position of facing conflicting cybersecurity reporting directives from several government entities. There needs to be more assertive streamlining of cybersecurity incident reporting policies to enable businesses to understand and follow clear and consistent guidelines and requirements. CIRCIA calls on the national cyber director (NCD) to lead an intergovernmental Cyber Incident Reporting Council composed of the Office of Management and Budget, CISA, and sector risk management agencies "to coordinate, deconflict, and harmonize" federal incident reporting requirements, including those issued through regulations. Considering CIRCIA, the SEC should collaborate with other federal agencies and cybersecurity policymakers, including the NCD, to both coordinate its proposed rules with other authorities and determine whether its requirements are advisable as written.

- **Company boards should prioritize managing cyber risks but not through SEC mandates requiring cybersecurity "expertise."** Our associations advocate for companies to proactively prioritize cyber risk management activities, but they are concerned about the SEC's call for companies to disclose the name of any board member who has cybersecurity expertise. We believe that board experts should not proliferate via government directives. Prescriptive disclosures intended to drive company behavior regarding which subject-matter experts sit on companies' governing bodies could lead to unwieldy and unwanted outcomes (e.g., giving investors a false sense of confidence because of the presence of a board cybersecurity "expert").

  Also, cybersecurity talent is scarce globally. It is unclear where companies would get the cybersecurity experts that would be driven by the Commission's proposed requirement to disclosure such expertise. There is a well-established lack of cybersecurity talent for the public and private sectors that would impede companies' abilities to recruit board cybersecurity experts. The SEC's proposal could even create unintended barriers for historically underrepresented groups to move into cybersecurity management or board leadership roles—not due to the lack of qualifications but to the absence of formal credentials (e.g., owing to their costs) and other certifications. Even if companies could obtain the relevant cybersecurity experts for board positions, no evidence has been

convincingly shown that this requirement would inform investors or improve companies' cybersecurity preparedness.

It is unlikely that even organizations such as NIST could readily pinpoint what constitutes expertise or experience in cybersecurity that would earn widespread agreement among industry professionals. Advancements in cybersecurity occur rapidly. Overseeing internal and external experts who are current in the field is more valuable than directors having outdated credentials. The SEC should accommodate a broader array of experiences than what the proposed rules' list of cybersecurity expert criteria encompasses. Consider Item 407's definition of an audit committee financial expert. It indicates, for example, that while a chief executive officer may not simultaneously serve as the company's accountant, this person may serve as an audit committee financial expert on the board because he or she has experience overseeing the accounting function at the company. Likewise, a suitable board cybersecurity expert may come from company management and not have formal schooling or training, but this individual understands cybersecurity practices and/or has experience supervising the company's personnel who are engaged in cybersecurity activities.

- **The term "cybersecurity incident" should be narrowed to correspond with significant incidents that do actual harm and existing definitions.** The scope of the SEC's definition of a cybersecurity incident is overly expansive. It should not be "construed broadly," as the Commission suggests. For reasons of consistency, agencies should avoid defining terms through their own processes. A reportable cybersecurity incident should track more closely with a "covered cyber incident" in CIRCIA or *Presidential Policy Directive, United States Cyber Incident Coordination* (PPD 41). PPD 41 refers to a "significant cyber incident" as a cyber incident that is "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." Material cybersecurity disclosures should correspond to significant incidents that do actual harm.

  In addition, companies need clarity in reporting requirements, which should be targeted to clear, objective criteria in any rule that the SEC—with industry input—develops. The definition of a cybersecurity incident, as currently written, would lead to the overreporting of cybersecurity incidents and not serve investors' decision making well.

Our organizations support responsible and protected cybersecurity reporting to the government, consumers, and investors, but we oppose the SEC's proposed rules as written. The proposal runs counter to sound cybersecurity policies and practices. It should be revised to better balance transparency with cybersecurity. We are ready to work with the Commission to develop a rulemaking that provides timely information to investors while mitigating risks associated with disclosing sensitive cybersecurity information to the public.

Sincerely,

ACA Connects—America's Communications Association
ACT | The App Association
Agricultural Retailers Association (ARA)
Airlines for America (A4A)
Alliance for Automotive Innovation
American Chemistry Council (ACC)
American Council of Engineering Companies (ACEC)
American Council of Life Insurers (ACLI)
American Fuel and Petrochemical Manufacturers (AFPM)
American Gas Association (AGA)
American Petroleum Institute (API)
American Property Casualty Insurance Association (APCIA)
Biotechnology Innovation Organization (BIO)
Competitive Carriers Association (CCA)
Consumer Technology Association (CTA)
CTIA
Federation of American Hospitals
The Fertilizer Institute (TFI)
Global Business Alliance
Healthcare Information and Management Systems Society (HIMSS)
Information Technology Industry Council (ITI)
Interstate Natural Gas Association of America (INGAA)
National Association of Broadcasters
National Association of Mutual Insurance Companies (NAMIC)
National Association of Chemical Distributors (NACD)
NCTA—The Internet & Television Association
National Electrical Manufacturers Association (NEMA)
NTCA—The Rural Broadband Association
Professional Services Council (PSC)
Securities Industry and Financial Markets Association (SIFMA)
Semiconductor Industry Association (SIA)
Telecommunications Industry Association (TIA)
U.S. Chamber of Commerce
USTelecom—The Broadband Association