November 1, 2022

Via: rule-comment@sec.gov

Ms. Vanessa A. Countryman
Secretary
Securities and Exchange Commission
100 F Street NE
Washington, DC 20549-1090

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

Dear Ms. Countryman:

The American Chemistry Council (ACC) submits these additional comments to the Securities and Exchange Commission (SEC) in response to the proposed rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure. I've attached ACC's comments submitted on May 9, 2022 in support of this letter.

To reiterate, ACC believes the SEC's 2018 guidance to publicly traded companies is sufficient in providing information on cybersecurity reporting obligations and provides information that informs investors. As proposed, SEC's cyber incident disclosure revisions could expose a company's security resilience procedures to cyber hackers. Materiality determinations are emphasized over cybersecurity risks. SEC's proposal would shift the focus to compliance-based reporting rather than the more appropriate focus on managing cyber risks and identifying and resolving cyber incidents.

The SEC proposal was drafted without the consideration of the cyber incident reporting requirements of other federal agencies and the newly enacted cyber incident reporting legislation. ACC members are subject to cyber-related rules required by the Department of Homeland Security, the Department of Energy, the Transportation Security Agency, the Department of Defense, the Environmental Protection Agency, and others, depending on the company's scope of activities. Rather than creating additional and potentially conflicting cyber incident reporting requirements, the SEC should coordinate with other federal agencies to harmonize reporting requirements.

Subject to the CISA rulemaking, the new cyber incident reporting legislation (CIRCIA) requires certain owners and/or operators of critical infrastructure to report "covered cyber incidents" to CISA within 72 hours. CIRCIA's 72-hour window compares roughly equally to the Commission's proposed Form 8-K requirement, which stipulates that a company must disclose a material cybersecurity incident to the SEC within 4 business days. However, the SEC

does not allow for temporary delays in reporting that may be due to internal investigation of the incident or external investigation, including efforts by law enforcement. Companies should not be required to report if it may compromise an ongoing investigation. The SEC should urge companies to work with law enforcement to mitigate cyber incidents, rather than disclose potentially inaccurate information within 4 business days.

Although a company may be able to make a materiality determination and subsequently disclose within four business days, in many cases it will not have the information necessary to make a meaningful disclosure within that time period. Cybersecurity incidents can take many months to investigate, with forensic analysis producing new information that likely alters factors relevant to the incident's technical and cybersecurity significance and broader business impact. Public disclosure of an unmitigated or uncontained cyber incident could lead to additional harm to investors. Cybercriminals often aim to embed themselves in corporate networks without the company knowing, sometimes for years. If the attack is discovered, additional harm could occur if the attack has not yet been contained or mitigated.

Requiring public disclosure of uncontained or unmitigated cyber incidents could distort the price of securities. By contradicting best practices for cyber incident response, the premature public disclosure of an incident may provide investors with an inaccurate measure of the company's true ability to respond to cybersecurity incidents. Premature disclosure during an early stage of the incident response process may result in investors receiving inaccurate information about the scope or impact of the incident.

SEC's proposal requires companies to disclose policies and procedures to "identify and manage cybersecurity risks and threats." Providing all the information required in this proposal (a detailed description of its cyber risk management program) could compromise a company's ability to defend against future cyber attacks. The SEC has not described why such a level of detail would benefit investors or that the benefits would outweigh the potential consequences to companies that are already victims of cybercriminals or nation state actors.

DHS-administered regulations that mandate the protection of cybersecurity-related information include the Chemical Facilities Anti-Terrorism Standards (CFATS) program and the Maritime Transportation Security Act (MTSA). CFATS information is safeguarded as Protected Critical Infrastructure Information, and MTSA information is safeguarded as sensitive security information. The SEC's proposed amendments are clearly at odds with the determination of DHS that information about cybersecurity incidents must be kept confidential and not publicly disclosed.

Cybersecurity talent is hard to find. From a personnel standpoint, it's unclear where companies would get the so-called cybersecurity expertise that the proposed regulation would mandate. There is a well-known lack of cybersecurity talent for the public and private sectors. In any case, the SEC has not justified that having cybersecurity experts on boards would benefit its cybersecurity protection program. Similarly, investors may see the inclusion of certain individuals on a company's board as an indication of a company's overall cybersecurity program

maturity and as a sign that a company is more secure than another one. Such an outcome could be misleading.

In summary, ACC urges the SEC to significantly revise this proposed rule or maintain the 2018 interpretive guidance. Please contact me at [redacted] with any questions regarding this submission.

Sincerely,

Bill Gulledge

Bill Gulledge
Senior Director, Chemical Products & Technology Division

May 9, 2022

Via: rule-comment@sec.gov

Ms. Vanessa A. Countryman
Secretary
Securities and Exchange Commission
100 F Street NE
Washington, DC 20549-1090

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

Dear Ms. Countryman:

The American Chemistry Council (ACC) submits these comments to the Securities and Exchange Commission (SEC) in response to the proposed rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure. The proposed revisions to the 2018 reporting requirements have significant potential major impacts on publicly traded companies, investors, and corporate governance programs.

ACC, in its letter dated May 2, 2022, urged the SEC to extend the comment period by an additional 30 days. The SEC did not approve this request. With the denial, ACC will not respond to the individual questions posed by the SEC in its current request, but the underlying reasons for the request remain:

"The proposed amendments to the 2018 reporting requirements have significant potential major impacts on publicly traded companies, investors, and corporate governance programs. Identifying issues and preparing comments to respond to 40 or so questions require considerable thought and resources to prepare useful responses. In addition, we note that the SEC is proposing several other significant notification rules, i.e., climate change, which have overlapping comment periods."

SEC's proposed revisions would require near real-time and periodic reporting of material cybersecurity incidents. The SEC proposal also requires companies to disclose procedures to address cyber risk, management's role, and expertise in implementing a cyber protection program, and disclosure of the company's board of director's role and expertise on cybersecurity. The information on material cyber incidents would be reported on Form 8-K.

ACC believes the SEC's 2018 guidance to publicly traded companies is sufficient in providing information on cybersecurity reporting obligations and provides information that informs investors. As proposed, SEC's cyber incident disclosure revisions could expose a

company's security resilience procedures to cyber hackers. Materiality determinations are emphasized over cybersecurity risks.

ACC, through its Responsible Care program, CFATs risk management and reporting requirements, and voluntary cyber risk management initiatives, emphasizes tiered risk management approaches to developing, maintaining, auditing, and revising cyber protection programs. The NIST cyber framework and industry standards and guidelines help form the foundation for these programs. SEC's proposal would shift the focus to compliance-based reporting rather than the more appropriate focus on managing cyber risks and identifying and resolving cyber incidents.

The SEC proposal was drafted without the consideration of the cyber incident reporting requirements of other federal agencies and the newly enacted cyber incident reporting legislation. ACC members are subject to cyber-related rules required by the Department of Homeland Security, the Department of Energy, the Transportation Security Agency, the Department of Defense, the Environmental Protection Agency, and others, depending on the company's scope of activities. Rather than creating additional and potentially conflicting cyber incident reporting requirements, the SEC should coordinate with other federal agencies to harmonize reporting requirements. SEC's current proposals could potentially interfere with law enforcement investigations of cyber crimes by diverting corporate and law enforcement resources from investigating and resolving significant cyber incidents.

SEC proposed to amend Form 8-K to require a company to disclose information about a cybersecurity incident within 4 business days after the company determines that it has experienced a "material" cybersecurity incident. The SEC argues that such reporting would "significantly improve the timeliness of cybersecurity incident disclosures, as well as provide investors with more standardized and comparable disclosures."

Specifically, a company would be required to disclose the following information about a material cybersecurity incident at the time of the Form 8-K filing—

- When the incident was discovered and whether it is ongoing.
- A brief description of the nature and scope of the incident.
- Whether any data was stolen, altered, accessed, or used for any other unauthorized purpose.
- The effect of the incident on the registrant's operations.
- Whether the registrant has remediated or is currently remediating the incident.

The disclosure requirement of 4 business days could require a company to report while the incident is still ongoing and being managed by the company and/or law enforcement. This could potentially provide attackers with additional information over company cyber defenses. Companies will have to determine whether a disclosure to SEC would negatively impact its cyber defense program and whether releasing security program information that is considered

confidential by the company will increase its risk to cyber attacks. If companies are required to report detailed information, the disclosure could provide a roadmap to vulnerabilities if malicious actors detected patterns.

Subject to a CISA rulemaking, the new cyber incident reporting legislation (CIRCIA) requires certain owners and/or operators of critical infrastructure to report "covered cyber incidents" to CISA within 72 hours. CIRCIA's 72-hour window compares roughly equally to the Commission's proposed Form 8-K requirement, which stipulates that a company must disclose a material cybersecurity incident to the SEC within 4 business days. However, the SEC does not allow for temporary delays in reporting that may be due to internal investigation of the incident or external investigation, including efforts by law enforcement. Companies should not be required to report if it may compromise an ongoing investigation. The SEC should urge companies to work with law enforcement to mitigate cyber incidents, rather than disclose potentially inaccurate information within 4 business days.

ACC members frequently hear from the FBI and DHS/CISA that notifying them is key toward mitigating cybersecurity incidents. Authorities can often figure out the details of a cybersecurity incident—the what, the when, and the how—as the incident moves forward, but the advantages of time and dialogue are important. Companies need time, potentially more than a few business days, to provide law enforcement with key information. The SEC reporting time requirement could undermine the public/private collaboration. Where a federal regulation exists, the SEC should reconsider its position on exemptions and incorporate into its proposed rule an exemption for entities that are subject to and in compliance with similar federal reporting regulations.

The SEC also proposes that companies disclose when a series of undisclosed individual immaterial cyber incidents become material in the aggregate. ACC believes that further guidance is required to determine when a series of incidents become material. Potential material incidents would be difficult to track over an undefined period.

SEC's proposal requires companies to disclose policies and procedures to "identify and manage cybersecurity risks and threats." Providing all the information required in this proposal (a detailed description of its cyber risk management program) could compromise a company's ability to defend against future cyber attacks. The SEC has not described why such a level of detail would benefit investors or that the benefits would outweigh the potential consequences to companies that are already victims of cybercriminals or nation state actors.

DHS-administered regulations that mandate the protection of cybersecurity-related information include the Chemical Facilities Anti-Terrorism Standards (CFATS) program and the Maritime Transportation Security Act (MTSA). CFATS information is safeguarded as Protected Critical Infrastructure Information, and MTSA information is safeguarded as sensitive security information. The SEC's proposed amendments are clearly at odds with the determination of

DHS that information about cybersecurity incidents must be kept confidential and not publicly disclosed.

This SEC proposal also requires disclosure of a company's cybersecurity governance, including Board oversight of cybersecurity risk and a description of management's role in assessing and managing cyber risks. The proposal would require companies to disclose whether they have a chief information security officer (CISO), his or her relevant expertise, and where the CISO fits in the entity's organization. The proposal would also require disclosures about the interactions of management and the board on cybersecurity, including the frequency with which the board and management considers cybersecurity risk and related topics. In addition, SEC's proposal says. "If any member of the board has cybersecurity expertise, the registrant would have to disclose the name(s) of any such director(s) and provide such detail as necessary to fully describe the nature of the expertise."

ACC believes these proposed requirements dictate that companies take specific cybersecurity actions that are not promoting sound cyber risk management practices and puts the SEC in the position to dictate how companies operate their cybersecurity protection programs. ACC also objects to disclosing the names of board members with cybersecurity "expertise." The SEC should not have any influence on which experts sit on a company's governing body.

Cybersecurity talent is hard to find. From a personnel standpoint, it's unclear where companies would get the so-called cybersecurity expertise that the proposed regulation would mandate. There is a well-known lack of cybersecurity talent for the public and private sectors. In any case, the SEC has not justified that having cybersecurity experts on boards would benefit its cybersecurity protection program. Similarly, investors may see the inclusion of certain individuals on a company's board as an indication of a company's overall cybersecurity program maturity and as a sign that a company is more secure than another one. Such an outcome could be misleading.

In summary, ACC urges the SEC to significantly revise this proposed rule or maintain the 2018 interpretive guidance. Please contact me at [redacted] with any questions regarding this submission.

Sincerely,

Bill Gulledge

Bill Gulledge
Senior Director, Chemical Products & Technology Division