



August 14, 2023

The Honorable Gary Gensler
Chair
U.S. Securities and Exchange Commission
100 F Street NE
Washington, DC 20549

Re: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (Release No. 33-11216)

Dear Chair Gensler:

The U.S. Chamber of Commerce (the “Chamber”) submits this letter in response to the recent rule adopted by the Securities and Exchange Commission (“SEC”) regarding cybersecurity incident reporting and cybersecurity practices by public companies (the “Rule”).¹ Cyber security is a priority for the Chamber and its members. While the Chamber appreciates some of the changes made to the March 2022 proposal, the SEC was dismissive of important issues raised by the Chamber and others.² The Rule creates procedures that are vague and unworkable, ignores the role of national security agencies, and establishes conflicting obligations on the part of the issuer leading to unclear enforcement standards. Unfortunately, many of these issues could have been addressed through historic deliberative processes used by the SEC for decades—such as roundtables and more extensive comment periods.

The SEC has chosen speed over accuracy, ignored the role of nation-state actors, and is forcing businesses to choose between disclosure and national security. The rule as it stands will degrade investor protection, capital formation and competition. Accordingly, the Chamber would recommend that the following steps be taken:

1. Delay the effective date by twelve months;
2. Hold a roundtable with general counsels, chief information officers, investors and other stakeholders to identify the foreseen and unforeseen adverse consequences of the Rule and craft solutions to the challenges identified;

¹ Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 88 Fed. Reg. 51896 (SEC August 4, 2023).

² See: Letter from Thomas Quaadman and Christopher Roberti, et. al, of the U.S. Chamber of Commerce to the SEC re: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (File Number 27-09-22). P. 8-9; 16-17; 26-27. Available at: <https://www.sec.gov/comments/s7-09-22/s70922-20128398-291304.pdf>

3. Develop guidelines with the Department of Justice and then establish and test the Attorney General mechanism to delay reporting, which will provide certainty to the business community and marketplace;
4. Convene, in an appropriate setting, a meeting with general counsels, chief information officers, investors and appropriate members of the national security community to establish a mechanism, as was done with the Department of Justice, to allow for disclosure, if appropriate, should a business be attacked by a nation-state actor;
5. Clarify the broad definition of cyber incident and to provide clear guidelines for enforcement proceedings; and
6. Take additional steps to minimize information flows that may benefit hackers.

We believe these steps, if taken expeditiously, can address many of the severe consequences that would ensue if the Rule were implemented as-is. Our concerns are outlined in more detail below.

The adopting release states that the Rule is intended to facilitate “timely, standardized disclosure” by companies to make it easier for investors to understand and assess the implications of a cyber incident or the effectiveness of a company’s cybersecurity practices. However, important provisions of the Rule rely on ambiguous, untested processes or require real-time, forward-looking disclosure as part of the new Form 8-K.³ It is imperative for companies to fully understand how the SEC intends to administer these provisions given that many registrants are expected to comply with aspects of the Rule by December 2023.

For example, the Rule stipulates that companies would have an additional thirty days to file a Form 8-K regarding a cybersecurity incident if the United States Attorney General determines that the disclosure “poses a substantial risk to national security or public safety.” Companies may receive additional time if the Attorney General makes the same determination before the end of the initial 30-day period.

Yet the Rule fails to address several commenters’ reservations regarding the Department of Justice (DOJ) making this determination. It is impossible to predict the timing, scope, and circumstances surrounding material cyber incidents, which can affect individual companies or groups of companies across industries. Accordingly, in many cases it may not be

³ See: Remarks from Commissioner Mark T. Uyeda. “Statement on the Final Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure.” July 26, 2023. Available at: <https://www.sec.gov/news/statement/uyeda-statement-cybersecurity-072623>

possible for the DOJ to make such a determination within the four-day period before a Form 8-K must be filed.

Moreover, other federal agencies are typically the lead agencies regarding major cyber incidents, so DOJ may not be in the best position to determine whether a disclosure poses a national security risk. Indeed, if a business is attacked by a nation-state actor or proxy, businesses will often have to rely on the national security structure to address the immediate issues and ensure that the larger issues are addressed.

The SEC dismissed, or ignored, these concerns in the adopting release without adequate justification.

When Commissioner Peirce raised these same questions during the July 26th SEC open meeting, staff simply referred to the “interagency communication process” as the mechanism that will ostensibly remedy any delays or issues that arise from DOJ making a national security determination. This “interagency communication process” – which appears to be a critical component of the Rule – receives only a passing mention in the adopting release, and no details are provided about specific staff at the SEC and DOJ that will be involved in the process, the timeframe for when SEC and DOJ commence their communication once a company has made a materiality determination, whether companies are expected to communicate directly with DOJ during the four-day period prior to a possible 8-K filing, or the expected response time within the four-day window to alert companies that a 30-day extension will be provided. Outstanding questions such as these should be clarified prior to December 18, 2023.

Moreover, the requirement that companies make a materiality determination “without unreasonable delay” could compel registrants to make assumptions about the scope of a specific attack and whether the attack will rise to the level of a “material” event. Mandating that such a determination be made within a short timeframe while a cyber incident is evolving again demonstrates the flaws of the Rule and potential problems with the materiality analysis prescribed by the SEC.

The Rule specifically states that the definition of “cybersecurity incident . . . is to be construed broadly.” The SEC must make clear how it intends to apply this definition in enforcement proceedings. This open-ended definition creates substantial uncertainty, particularly as it concerns “a series of related unauthorized occurrences,” as to the scope of the rulemaking.

The Chamber and its members would welcome the opportunity to work with the SEC to gain a better understanding of how the SEC plans to implement and administer the Rule. Given what is at stake with the Rule in terms of investor protection and the national security and public safety issues it implicates, we believe it is important for companies to have a full understanding of compliance expectations. We appreciate the SEC’s consideration of this request and look forward to our ongoing dialogue with commissioners and staff on these important matters.

Sincerely,



Tom Quaadman
Executive Vice President
Center for Capital Markets
Competitiveness
U.S. Chamber of Commerce



Christopher Roberti
Senior Vice President
Cyber, Intel, and Supply Chain
Security Policy
U.S. Chamber of Commerce

cc: The Honorable Hester Peirce, Commissioner
cc: The Honorable Caroline Crenshaw, Commissioner
cc: The Honorable Mark Uyeda, Commissioner
cc: The Honorable Jaime Lizarraga, Commissioner
cc: Mr. Erik Gerding, Director, Division of Corporation Finance