**Chris Netram**

*Managing Vice President,*
*Tax and Domestic Economic Policy*

May 9, 2022

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

Re: File No. S7-09-22; Release Nos. 33-11038, 34-94382, IC-34529: *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*

Dear Ms. Countryman:

The National Association of Manufacturers ("NAM") appreciates the opportunity to provide comment to the Securities and Exchange Commission ("SEC") on File No. S7-09-22, the Commission's proposed rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure.[1]

The NAM is the largest manufacturing trade association in the United States, representing manufacturers of all sizes and in all 50 states. Manufacturing is a capital-intensive industry, requiring significant investments for equipment purchases and research and development. Manufacturers often turn to the public capital markets to finance these pro-growth activities, which set the stage for economic expansion, innovation, and job creation. Thus, a vibrant public market that supports capital formation and long-term growth is critical to the sustained success of manufacturing in America.

Manufacturers of all sizes and in all sectors know that protecting their business—and thus the investors that provide much-needed capital to support manufacturing growth in the United States—from cybersecurity risk is critical for success in today's economy. Through comprehensive and connected relationships with customers, vendors, suppliers, and governments, manufacturers maintain highly sensitive data and valuable intellectual property. The responsibility of securing information, networks, facilities, and machinery that support manufacturing is a top priority for our sector. Further, manufacturers know that disclosing material information about these important practices is vital to informing and protecting shareholders in publicly traded companies.

The NAM appreciates that the SEC's proposed rule is designed to elevate the importance of cybersecurity risk management at public companies. Shareholders in all businesses benefit when public companies take appropriate steps to guard against cybersecurity risk. Cyber criminals, nation state attackers, and other hackers continue to employ increasingly sophisticated methods to infiltrate and attack businesses and steal data, and manufacturers are leading the way in continuing to evolve their defenses in response to these threats. The NAM recognizes and appreciates the importance of adopting these critical cybersecurity practices and of reporting material information about cybersecurity risk management and cybersecurity incidents to investors.

However, we are concerned that some of the requirements in the proposed rule could be needlessly burdensome and duplicative for public companies given the existing layers of federal cybersecurity

[1] *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, 87 Fed. Reg. 16590 (23 March 2022). Release Nos. 33-11038, 34-94382, IC-34529; *available at* https://www.govinfo.gov/content/pkg/FR-2022-03-23/pdf/2022-05480.pdf.

reporting already in existence. Further, some of the proposed disclosures could ultimately endanger shareholder value by publicly exposing sensitive information, including to the bad actors that threaten companies' cybersecurity on a daily basis.

The SEC's proposed disclosure regime is a departure compared to other agencies' cybersecurity reporting requirements in that the reports would be publicly available. In most situations, public reporting fits squarely within the SEC's mission to protect investors via material disclosures; however, in the cybersecurity context such reporting brings additional risks for those same investors. If the SEC's disclosure mandate exposes sensitive information about a company's cybersecurity protections, reveals data about what types of attacks are successful, interferes with a law enforcement investigation into a cybersecurity incident, distracts a company from responding to an ongoing threat, or endangers the national security of the United States, do investors ultimately benefit from the disclosure? Premature public disclosure of sensitive information about an incident or a vulnerability contradicts well-established best practices for cybersecurity because such disclosure can enable attackers at a time when a company is potentially at its most vulnerable. As such, the NAM is hopeful that any final SEC rule will provide companies with the flexibility to balance the need for prompt reporting against the risks inherent in exposing sensitive cybersecurity information to the public.

As the SEC works to finalize its proposed rule on cybersecurity disclosures, the NAM respectfully encourages the Commission to take steps to balance the risks and benefits of any new reporting requirements. We also urge the SEC to collaborate with other federal agencies with cybersecurity expertise in order to ensure that the government's cybersecurity reporting obligations align to the largest extent possible—and so that the SEC is fully aware of the impacts that a public reporting requirement could have on companies' cybersecurity defenses and the United States' national security. Appropriate flexibility will allow manufacturers to protect themselves against cybersecurity risks, provide timely and accurate cybersecurity disclosures to their investors, and safeguard sensitive information.

## I. The SEC should incorporate the principles-based approach outlined in its 2018 guidance into any new cybersecurity reporting requirements.

In 2018, the SEC promulgated interpretative guidance related to public company cybersecurity disclosures.[2] At the time, the Commission underscored the "increasing significance of cybersecurity incidents"[3] and "stresse[d] the importance of maintaining comprehensive policies and procedures related to cybersecurity risks and incidents."[4] The NAM strongly agreed, and continues to agree, with this assessment. The 2018 guidance also noted that it is "critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion."[5] Specifically, the guidance reminds public companies of their obligation to "provide timely and ongoing information in [Forms 10-K and 10-Q] periodic reports regarding material cybersecurity risk and incidents"[6] and encourages issuers to use Form 8-K current reports to ensure that information about material cybersecurity incidents is disclosed promptly.[7] Again, the NAM supports and agrees with these standards.

---

[2] *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, 83 Fed. Reg. 8166 (26 February 2018). Release Nos. 33-10459, 34-82746; *available at* https://www.govinfo.gov/content/pkg/FR-2018-02-26/pdf/2018-03858.pdf.

[3] *Id.* at 8167.

[4] *Ibid.*

[5] *Ibid.*

[6] *Id.* at 8168.

[7] *Ibid.*

In its 2018 guidance, the Commission outlined reasonable principles for disclosure and reminded public companies of their legal obligations to keep investors well-informed about cybersecurity risks and incidents. Given public companies' ongoing usage of and reliance on the 2018 guidance, it is not immediately clear why a new cybersecurity disclosures rule is necessary. Although the cybersecurity threat landscape has continued to evolve and change since 2018, the guidance's principles-based approach was designed to account for just such an evolution. The NAM is concerned that the SEC has proposed a significantly more prescriptive approach than the one described as requiring companies to establish "robust disclosure controls and procedures"[8] by the Commission just four years ago. The NAM supports these robust controls and procedures—and manufacturers' critical efforts to combat cybersecurity threats while providing timely and accurate cybersecurity disclosures to their investors.

The 2018 guidance repeatedly underscores the requirement that public companies keep investors informed about cybersecurity risks and material cybersecurity incidents. The guidance suggests specific practices for appropriate cybersecurity reporting—without mandating detailed line-item disclosures or instituting hard deadlines for companies to meet. The NAM believes the approach outlined in the 2018 guidance is sufficient to inform investors about and protect investors from cybersecurity risk. As the SEC works to finalize its proposed rule, we respectfully encourage the Commission to incorporate the guidance's principles-based approach into any new cybersecurity reporting requirements and to avoid one-size-fits-all mandates that may do more harm than good.

## II. The SEC should coordinate with (and, as appropriate, defer to) federal law enforcement, cybersecurity, intelligence, and national security agencies as it works to finalize its proposed cybersecurity rule.

The SEC is not the first federal agency to promulgate cybersecurity reporting requirements. For example, surface transportation operators are subject to a Transportation Security Administration ("TSA") Security Directive that requires reporting cybersecurity incidents to the Cybersecurity and Infrastructure Security Agency ("CISA") within the Department of Homeland Security ("DHS").[9] Defense contractors face similar requirements to notify the Department of Defense ("DOD") after discovering a cybersecurity breach.[10] The National Institute of Standards and Technology ("NIST") maintains a cybersecurity framework to help companies understand and manage their cybersecurity risk.[11] Most recently, Congress enacted the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA"), which will require owners and operators of critical infrastructure—including many manufacturers—to provide cybersecurity incident reports to CISA.[12]

These reporting requirements differ from the SEC's proposed rule in several key ways. First and foremost, the reports submitted pursuant to these frameworks are confidential. They are designed to inform the relevant agency so that appropriate steps can be taken to respond to an ongoing breach or guard against future attacks. They do not suggest publicly sharing information about cybersecurity vulnerabilities. The SEC's incident reporting proposal, on the other hand, would mandate public disclosure of details about material cybersecurity incidents. While the NAM supports public

---

[8] *Id.* at 8167.

[9] *Enhancing Surface Transportation Cybersecurity*. Transportation Security Administration (31 December 2021). *Available at* https://www.tsa.gov/sites/default/files/20211201_surface-ic-2021-01.pdf.

[10] 32 CFR 236.4.

[11] *Framework for Improving Critical Infrastructure Cybersecurity*. National Institute of Standards and Technology (16 April 2018). *Available at* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[12] *See* Division Y, *Consolidated Appropriations Act, 2022*. P.L. 117-103.

disclosure of material information, it is still the case that public disclosures present significantly increased burdens and risks as compared to agency notifications—including the costs and legal liability associated with SEC filings and the potential dangers of exposing sensitive information to hackers. As such, the SEC should coordinate with its sister agencies and provide flexibility to companies in order to ensure that any required public reports do not expose businesses, investors, or the United States to increased cybersecurity risks. The NAM is concerned that the proposed rule's lack of flexibility and coordination could interfere with critical law enforcement investigations into cyber criminals and could be detrimental to the United States' national security.

Additionally, it is notable that the agencies overseeing the existing cybersecurity reporting frameworks have both the expertise and the statutory mandate to protect Americans and American businesses from harm. Given the wealth of expertise across the federal government on this critical issue, and the web of overlapping agency notification requirements to which businesses are already subject, the NAM respectfully encourages the SEC to closely coordinate with other federal agencies as it works to promulgate its own cybersecurity reporting requirement. In particular, the NAM is hopeful that the SEC will defer to CISA during the implementation of the new CIRCIA notification regime. The NAM has called for CISA to provide a "reasonable and flexible reporting deadline" that allows manufacturers to respond to "emerging information and other factors" when providing the required incident notifications.[13] CISA has two years to promulgate implementing regulations, and the NAM is concerned that the SEC's more-expedited timeline for its cybersecurity rule could result in divergent reporting requirements. Unfortunately, the SEC's expedited consideration of its proposed disclosure regime indicates that the first rule to be finalized likely will *not* be from the federal government's cybersecurity agency.

In addition to working with and deferring to CISA during the implementation of CIRCIA, the NAM respectfully encourages the SEC to coordinate with the Federal Bureau of Investigation ("FBI") and the Department of Justice ("DOJ") as to the impact of public disclosure on law enforcement investigations into cybersecurity incidents. We also encourage the Commission to engage with the National Security Agency ("NSA"), the Department of State, DOD, and DHS to understand the national security implications of the SEC's proposed rule. The NAM believes that these agencies' expertise and experience are critical to the success of any final SEC cybersecurity reporting rule.

## III. The SEC should allow for greater flexibility with respect to the proposed four-day reporting requirement for cybersecurity incidents in order to prevent harm businesses, shareholders, and national security.

The proposed rule would require public disclosure within four days of a public company determining that it has experienced a material cybersecurity incident. Under the rule, companies would be required to file a Form 8-K to describe the incident, report when it was discovered and whether it is ongoing, explain any effects on the company's operations, and provide additional information about the event and its impact. The NAM supports appropriate and timely disclosure of material incidents, but the proposed four-day requirement would increase costs and complexity for businesses, potentially mislead investors, and ultimately create significant risks for shareholders and the broader economy that would eclipse the potential benefits of reporting. We respectfully encourage the SEC to re-evaluate the proposed rule's one-size-fits-all four-day reporting requirement; at a minimum, the SEC should allow for reporting to occur after a company has had a reasonable opportunity to respond to and resolve an incident.

[13] NAM Letter on S. 2875 (5 October 2021). *Available at* https://www.nam.org/wp-content/uploads/2021/10/NAMSenateSHSGACLtrS.2875.pdf.

### A. The NAM appreciates that the proposed incident reporting framework would require disclosure only of material cybersecurity events and would start the disclosure clock for incident reports following the completion of a company's materiality determination.

#### *1. The SEC should maintain its proposed requirement that companies disclose only material cybersecurity events.*

The NAM appreciates that the proposed rule would require disclosure only of material cybersecurity incidents. In today's interconnected economy, cybersecurity attacks are far too common. Public companies must be prepared for a constant barrage of phishing attempts and potential minor intrusions. Yet these smaller attacks—both on their own and in the aggregate—are immaterial to a company's operations and financial condition. It would make little sense to require repetitive disclosures of inconsequential incidents that pose minimal risk to a business and its investors. As such, the NAM appreciates that the proposed rule's incident reporting obligations are targeted at only those incidents that are material to a company.

Further, the NAM appreciates that companies would retain the ability to classify an incident as material based on the well-understood definition of materiality expressed by the Supreme Court.[14] Bright-line materiality tests or SEC-mandated determinations that certain sizes or types of incidents would be *per se* material would oversimplify a complex issue and ultimately impose significant burdens on companies by requiring disclosure of incidents that may not be material to investors.[15]

Put simply, different sizes and types of incidents will impact companies in distinct ways, so it would be inappropriate for the SEC to promulgate a top-down standard that applies to all businesses and all areas of the economy. Issuers' materiality assessments will incorporate data on the size, scale, and scope of a particular incident alongside information about the business itself and the industry in which it operates, including the company's cybersecurity risk exposure, its relationships with customers, suppliers, and vendors, and its governance and risk management practices and procedures. The SEC should continue to allow companies the flexibility to incorporate these and other variables into the materiality analyses envisaged by the proposed rule rather than attempting to dictate a uniform definition of materiality.

#### *2. The SEC should continue to base any reporting deadlines on the completion of a company's materiality assessment.*

The proposing release solicits comment on whether there should be "a different triggering event" (as opposed to the completion of a company's materiality assessment) that would set the reporting deadline for the required incident disclosures. The release suggests that such a trigger could be a company's discovery of an incident about which it has not yet made a materiality assessment.[16] The NAM strongly supports the proposed reporting trigger (i.e., an issuer's determination that a given cybersecurity incident was material) and would oppose any changes that would set accelerated reporting deadlines based on the occurrence or discovery of an incident. Starting the disclosure clock based on any event other than a materiality determination could lead to costly and potentially risky disclosure obligations following even the most inconsequential of incidents.

---

[14] *See, e.g., TSC Industries, Inc. v. Northway, Inc.*, 426 U.S. 438 (1976); *see also Basic, Inc. vs. Levinson*, 485 U.S. 224 (1988).

[15] The proposing release solicits comment on whether the SEC should mandate disclosure based on a "quantifiable threshold" related to a company's assets, equity, revenues, or net income (*see* Proposed Rule, *supra* note 1, at 16597). The NAM would oppose such a bright-line test.

[16] Proposed Rule, *supra* note 1, at 16597.

Further, materiality analyses are often complicated and will take time to conduct, especially while a company is working to investigate, understand, respond to, and mitigate the impact of an incident. It would make little sense to force a rushed materiality assessment in the immediate hours after discovery of an attack by requiring disclosure four days after such a discovery. Investors will be much better served by the SEC's proposal to allow companies the necessary time to understand an incident and conduct a full and fair materiality assessment—and *then* to start the reporting clock that will ultimately result in Form 8-K filings about incidents determined to be material. The NAM respectfully encourages the SEC to maintain its proposed triggering event and to continue to emphasize the importance of company materiality assessments under any final rule.

### B. The proposed four-day reporting requirement would divert company resources from responding to an incident, result in potentially misleading disclosures for investors, and benefit bad actors.

Even assuming that the SEC maintains its proposed reporting trigger of a company's determination that an incident is material (rather than the discovery of the incident or its occurrence), the NAM is concerned that the proposed four-day reporting deadline could prove burdensome for public companies and, more importantly, could expose shareholders and the broader economy to risks that far outweigh any benefit of enhanced cybersecurity disclosure. The NAM respectfully encourages the SEC to reconsider its proposed one-size-fits-all four-day reporting deadline and instead look to provide more flexibility for companies to balance the benefits of timely reporting against the risks of premature disclosure.

The early days after discovery of a major cybersecurity incident are often characterized by confusion, incomplete data, and an all-hands-on-deck effort to investigate and respond to the threat. In some instances, the incursion or intrusion has not yet been contained—a process that can sometimes take weeks or months. Requiring a new, public report during this critical time would divert internal resources from responding to an attack; it could also result in misleading disclosures for shareholders or provide critical information to the perpetrators of the attack.

#### *1. Reporting within four days would impose significant burdens on public companies and hamper efforts to investigate and respond to an incident.*

Upon discovering a cybersecurity incident, a company must assess the significance of the event, identify the systems within the business that may have been compromised, and analyze the impact on its operations, customers, financial performance, and more. Companies may also work with law enforcement to determine the source of the attack and whether there are potential future vulnerabilities that the attack has exposed. In many instances, the attack will still be ongoing or its impacts will still be felt throughout this initial period of investigation and evaluation, so it is critical for the company to focus its resources on protecting the business as well as its customers, shareholders, and other partners (such as suppliers and vendors) during this time.

For major attacks, it may be clear relatively early that the incident is material—which, under the SEC's proposed rule, would begin the four-day clock counting down to the incident reporting deadline. The NAM is concerned that diverting time and resources away from understanding and responding to an incident and instead toward preparing an SEC filing would not be in the best interests of the shareholders the proposed rule is designed to protect. While timely disclosure about material incidents is important, an arbitrary four-day mandate could potentially harm shareholders by diverting resources from efforts to address the impact of an attack. These all-hands-on-deck mitigation efforts involve cybersecurity, risk management, IT, operations, management, and legal staff—in short, the exact individuals necessary to prepare an SEC filing about the incident. The NAM believes that investors would be better served if company staff and leadership and any external

consultants could focus solely on responding to an incident without needing to take time to produce an SEC filing based on an arbitrary deadline.

### *2. Premature incident reports could mislead investors in the early days following an attack.*

In addition to distracting issuers from responding appropriately to cybersecurity threats, a four-day incident reporting requirement could also result in potentially misleading disclosures for investors. The information available about an ongoing incident evolves rapidly in the early days after its discovery. The four-day reporting deadline would require disclosure of a company's perspective on an attack after 96 hours—even if its understanding of the incident is changing rapidly at the time the report is due (and would likely continue to evolve going forward). As such, the Form 8-K could potentially overstate or understate the risk posed by an incident given that companies may still be assessing the reach and impact of an attack in its early days. Investors making decisions to sell or short a stock based on overstated day four risks, or decisions to buy or hold a stock based on understated risks, would benefit from a company waiting to report an incident until it is comfortable that all relevant facts are available—flexibility which should be allowed under any final rule. Though the proposed rule allows for updates following a Form 8-K filing, these updates may not benefit investors who relied on the initial filing, and any updates would further divert resources from addressing the effects of an attack and restoring operations to their normal state.

In addition to potentially harming shareholders, the uncertainty inherent in making public filings on day four of an ongoing incident could also create significant litigation or reputational risks for companies. If reported information is incomplete or unclear (despite companies' best efforts to provide accurate disclosures), market participants may allege that the Form 8-K was materially misleading and pursue legal action. As such, if the SEC persists in mandating a four-day disclosure window, it should allow companies' incident reports to be furnished to rather than filed with the Commission. The proposing release solicits comment on whether incident disclosures could be furnished;[17] such a modification would at least reduce the legal liability for businesses, an impactful change given the uncertainty associated with making public reports in the heart of an evolving crisis. The NAM would also support a safe harbor for disclosures made in reasonable reliance on information provided by third parties. Of course, furnished disclosures and a third-party safe harbor would not alleviate the time and resources necessary to prepare a report during an ongoing incident, nor would they prevent bad actors from utilizing any reported information for nefarious purposes—but the reduced legal liability would at least mitigate one risk factor associated with the proposed rule.

### *3. The proposed definition of "information systems" would require disclosure of a wide range of incidents involving third party systems about which a company may have incomplete or inadequate information.*

The proposed rule defines a cybersecurity incident to include an "unauthorized occurrence on or conducted through a registrant's information systems."[18] "Information systems," in turn, are defined as information resources "owned or used" by the registrant.[19] The NAM believes this definition could create compliance difficulties given that a company may "use" many systems to process its data, including third-party vendor systems such as software-as-a-service, platform-as-a-service, or infrastructure-as-a-service offerings over which the company has no operational control.

---

[17] *Id.* at 16598.

[18] *Id.* at 16601.

[19] *Ibid.*

Companies often must rely on these vendors to inform them of the details of cybersecurity incidents impacting the vendors' systems. Under such circumstances, manufacturers may experience challenges in obtaining sufficient information from the vendors to make an informed materiality determination. Vendors may even be hesitant to promptly share detailed incident information due to liability or confidentiality concerns. This lack of information availability increases the risk that an issuer may be forced to rush to make a materiality determination based on limited information. The NAM believes it would be more appropriate for the definition of "information systems" to include just those resources that are "owned or *operated*" by a company (as opposed to "owned or used"). Such a clarification would make it more likely that companies would be able to obtain relevant and useful information about an incident in a timely manner in order to conduct the required materiality assessment and file the required incident report.

#### *4. Requiring public reporting while an incident is ongoing could provide damaging information to the perpetrators of the attack and to other hackers.*

In addition to resource diversion and the potential for misleading disclosures, the most critical danger of an arbitrary four-day public reporting deadline is that the perpetrators of an attack will be able to read a company's disclosures alongside the rest of the public. Even the notice that a company has discovered an incident could be sufficient for a hacker to change tactics, either to escalate an ongoing attack against the company filing the SEC-mandated reports or to modify a strategy in another attack. Though the proposed rule notes that companies would not be required to disclose technical information about an attack, there is nevertheless still a risk that hackers could utilize any information reported to their advantage—and thus to the detriment of the company and its shareholders.

Caution is warranted in the days immediately following discovery of an incident (especially when the incident is still ongoing), yet the proposed rule's four-day clock does not allow for any flexibility or reporting delay—even when it might be beneficial to the company, its investors, and the broader marketplace. For example, a common practice in the event of an incident related to a service provider is to notify the provider first, in confidence, so they can patch the vulnerability for their other clients. But under the proposed rule, companies would not be allowed to delay their Form 8-K to wait on the patch, potentially exposing the broader economy to a much higher degree of risk by allowing hackers to stay one step ahead of any mitigation efforts. The public nature of these disclosures (as compared to the confidential filings that companies are required to make to CISA and other agencies) means that investors and hackers will be notified of any ongoing incidents at the exact same time. Early notifications to CISA or DOD can enable those agencies to assist with mitigating an ongoing incident—whereas early disclosures to the public (including the hackers perpetrating the incident) could have the opposite effect, ultimately increasing risks to investors.

### C. The SEC should abandon its proposed four-day reporting regime in favor of a flexible reporting requirement that enables timely disclosure of material cybersecurity incidents.

Given the risks to shareholders posed by a four-day disclosure requirement, the NAM respectfully encourages the SEC to allow for greater flexibility with respect to the reporting deadline for material cybersecurity incidents. The public nature of any SEC-mandated disclosures combined with the short reporting window could make the proposed rule's incident reporting requirement difficult and dangerous—but targeted amendments to the proposal can meet the SEC's stated goals while still protecting investors.

In 2018, the SEC made clear that companies should use Form 8-K to disclose material information about cybersecurity information "promptly"[20] and emphasized the importance of "accurate and timely disclosure of material events."[21] The NAM believes that a standard based on accurate and timely reporting would be sufficient to protect investors—while substantially mitigating the risks to investors posed by premature public disclosure. Perhaps the SEC could provide guidance as to factors that companies should consider in evaluating the timeliness of their reports, or suggest best practices to encourage appropriately prompt disclosures. Such advice could ease compliance for businesses and ensure that investors are receiving material information about cybersecurity incidents within an appropriate timeframe. But the NAM does not believe that a one-size-fits-all four-day reporting requirement is necessary or reasonable.

Companies need flexibility to appropriately balance shareholders' need for prompt disclosure with their need to be protected from ongoing and future attacks. A principles-based requirement that emphasizes the importance of timely disclosure without imposing a top-down mandate based on a specific number of days would more accurately reflect the evolving nature of cybersecurity risk and of individual cybersecurity incidents. The NAM respectfully encourages the SEC to reconsider its proposed four-day incident reporting mandate and instead to institute a principles-based requirement that provides information to shareholders on a timely basis while still allowing companies the requisite flexibility to protect investors from the significant risks of premature disclosure.

### D. The SEC should allow companies to delay incident reports if premature disclosure would interfere with an ongoing law enforcement investigation or otherwise impact public safety.

Companies do not respond to cybersecurity incidents in isolation. In many cases—especially significant breaches that would necessitate Form 8-K disclosure—businesses work closely with law enforcement to investigate an incident. Local, state, and federal authorities are critical to companies' efforts to understand the scope of an incident and take steps to protect any impacted businesses, employees, or customers; these authorities also conduct the official investigation into an incident and work to apprehend its perpetrators. A strong partnership with the relevant law enforcement agencies is critical to combatting an ongoing incident and to potentially recouping losses after an event has been contained. Yet, as Commissioner Peirce noted, the proposed rule is "unduly dismissive of the need to cooperate with, and sometimes defer to, [the SEC's] partners across the federal government and state government."[22] The NAM respectfully encourages the SEC to allow reporting flexibility for companies engaged with law enforcement in response to a cybersecurity attack. We further urge the SEC to work closely with the FBI and the DOJ to understand the potential risks to law enforcement investigations posed by premature public disclosure of cybersecurity incidents and to amend its proposed reporting requirement accordingly.

While the NAM supports timely disclosure of information about material cybersecurity incidents, in certain instances it may be more beneficial to investors for companies *not* to disclose an incident immediately if doing so would interfere with an ongoing law enforcement investigation. The proposing release is cognizant of this dynamic, acknowledging that "a delay in reporting may facilitate law enforcement investigations aimed at apprehending the perpetrators of the cybersecurity incident and preventing future cybersecurity incidents."[23] Yet the proposed rule would not allow for

---

[20] 2018 Guidance, *supra* note 2, at 8168.

[21] *Id.* at 8167.

[22] *Dissenting Statement on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Proposal*. Commissioner Hester M. Peirce (9 March 2022). *Available at* https://www.sec.gov/news/statement/peirce-statement-cybersecurity-030922.

[23] Proposed Rule, *supra* note 1, at 16596.

any flexibility if, in law enforcement's expert opinion, delaying public disclosure would enable them to better identify or apprehend wrongdoers or to protect the public from ongoing or future attacks.

Working with law enforcement, companies need the flexibility to balance the importance of prompt disclosure against any risks law enforcement identifies with respect to an ongoing investigation. The NAM understands and acknowledges that law enforcement investigations are often lengthy, so we are not suggesting that a *carte blanche* exemption is necessary to provide flexibility for companies to appropriately defer to law enforcement and protect their investors. However, the NAM strongly believes that companies should be allowed to balance the pros and cons of disclosure in the immediate aftermath of a cybersecurity incident and to make a determination as to the appropriate timeline for disclosure in consultation with the federal and state agencies investigating an attack. We respectfully encourage the SEC to reconsider its decision not to allow for any reporting flexibility even when law enforcement believes it would be in the best interest of an investigation. The ability to delay reporting until the danger has passed would be a commonsense allowance that would not undercut the efficacy of the proposed reporting requirement. In fact, such an allowance would ultimately benefit shareholders, who would be better served by a successful investigation that apprehends the perpetrator and protects the company and the economy from future attacks than they would by a top-down reporting obligation that could endanger their investments further.

Similarly, companies in certain critical industries should be able to temporarily delay reporting in consideration of issues related to public safety. Premature disclosure could lead individuals to make health- or safety-related decisions based on incomplete information, such as deferring medical procedures or disconnecting certain types of devices. It can take significant time and effort, often alongside government authorities, to understand the scope of an incident, develop the correct fix for a vulnerability, and determine how to safely implement any necessary modifications. Companies also must work with the government to decide how best to communicate the appropriate information about health- and safety-related incidents to the public. Public safety, including patient safety, must be the top concern following cybersecurity incidents—so the NAM supports appropriate flexibility with respect to the SEC's reporting deadline.

The proposing release does solicit comment on whether the Attorney General should be able to request that a company delay reporting if such a delay would be "in the interest of national security." The NAM appreciates that the SEC is cognizant of the potential risk to national security, which we discuss in further detail below. And we also appreciate the suggestion that the DOJ could have a unique perspective on the appropriateness of making public certain information about critical cybersecurity incidents. However, the risks to investors posed by premature disclosure extend beyond just information that might implicate the United States' national security. As discussed, publicly reporting information about an ongoing attack or investigation could interfere with law enforcement's efforts to identify the perpetrator or recoup losses. These are critical goals, even if they do not rise to the level of a national security threat. Reporting delays should be available to companies in these instances; however, the NAM does not believe that businesses should be required to obtain a written determination from the Attorney General within four days in order to qualify for a delay. Rather, companies should be allowed to coordinate closely with the DOJ and the FBI (and/or other federal, state, and local law enforcement agencies) and make a holistic assessment as to the risks posed to the business and the broader marketplace by premature public disclosure. The NAM supports a flexible SEC reporting requirement that allows for needed delays while still underscoring the importance of timely and accurate disclosure.

### E. The SEC should provide an explicit reporting exemption for classified information and should allow companies to delay or forgo incident reports if necessary to protect the national security of the United States.

In some instances, the risk of premature disclosure is broader than the potential impacts on an individual company and its investors. For many businesses that work with the federal government, including those that contract with or are subject to regulations promulgated by agencies like DOD, DHS, and the State Department, reporting information about a cybersecurity incident could implicate classified information or endanger the United States' national security.

Businesses that contract with the federal government are trusted with a range of sensitive information, and they are subject to strict rules (including criminal statutes) regarding the use and disclosure of this information. Similarly, businesses subject to DHS security regulations are prohibited from disclosing information about the operations of and materials stored in their facilities. As proposed, the SEC's cybersecurity incident reporting framework does not provide any flexibility with respect to sensitive or classified information. If a breach were to implicate a classified program, impact a classified facility, or involve classified information, public companies would be put in the untenable position of choosing between violating an SEC rule requiring disclosure and criminal statutes or other regulations prohibiting it.[24] Public disclosure of classified information (or, similarly, reports that allude to or implicate classified information even if not fully disclosing the information itself) creates legal risk for companies and potentially endangers all Americans. Classified information is classified for a reason, and the SEC should not require public companies to publish information that could put Americans at risk—even in service of shareholder transparency. The NAM strongly encourages the SEC to be explicit that public companies would be under no obligation to disclose classified information nor to violate any laws or agreements with respect to classified contracts, programs, or facilities. It is in the best interests of all Americans for such information to be fully exempt from the proposed disclosure requirement.

Further, businesses experiencing a cybersecurity incident may have access to information critical to national security that is not specifically classified. The existence of the attack itself also may implicate national security. For instance, suppose an incident is perpetrated by a foreign adversary of the United States—an increasingly common dynamic in today's geopolitical climate. A company experiencing such an attack should be allowed to first notify DOD, DHS, NSA, and/or the State Department and then defer to the judgement of the relevant agency as to the appropriateness of public disclosure about the incident, even if the incident may be material to shareholders. When cybersecurity incidents impact the United States' national security, or when disclosure of these incidents could have the potential to do so, companies should not be hamstrung by a public reporting obligation promulgated by the SEC. Instead, they should have the flexibility to delay or forgo reporting in order to safeguard the United States' national security and protect all Americans from potential harm.

The proposing release is at least cognizant of this risk, soliciting comment on whether companies should be allowed to delay reporting if the Attorney General determines that disclosure would impact national security. Though the DOJ and the law enforcement agencies it oversees (particularly the FBI) will undoubtedly play a role in helping companies understand the scope of an attack, including whether an incident implicates national security-related information or was perpetrated by a foreign adversary or its affiliates, the proposing release's focus on the Attorney General as the sole arbiter of national security decisions is misplaced. Depending on the incident, DOD, DHS, NSA, or the State Department would likely have a more helpful perspective on the national security ramifications of

[24] We would further note that obligations to avoid disclosure of classified information can extend beyond the United States. Many multinational businesses may be subject to state secret laws outside of the U.S., adding further complexity to the SEC's proposed reporting requirement.

premature disclosure and whether public reporting would violate existing laws or regulations. If a company believes that disclosure with respect to a cybersecurity incident could imperil the United States' national security, SEC rules should allow the company to coordinate with the relevant national security agencies and make an appropriate determination as to the timing and content of any public reports about the incident. The NAM respectfully encourages the SEC to defer to these agencies and their expertise in order to protect all Americans and the national security of the United States.

## IV. The SEC should rescind its proposed requirement that companies retrospectively analyze, aggregate, and potentially disclose the impact of previous immaterial cybersecurity incidents.

In addition to the current event reporting requirement for material cybersecurity incidents, the proposed rule would also require companies to provide disclosure "when a series of previously undisclosed individually immaterial cybersecurity incidents has become material in the aggregate."[25] The NAM opposes this requirement, which would impose a significant retrospective tracking and monitoring burden on companies without providing useful information to investors.

Immaterial incidents are by their very nature inconsequential to a business and its shareholders. Companies have processes and procedures in place to monitor and address these minor incidents, and they often take steps to identify patterns and guard against repeat attacks by the same or similar malicious actors. The number of minor incidents thwarted by company safeguards can reach the millions—but these unsuccessful attempts ultimately have little-to-no impact on a business. As such, it is not practical or helpful to investors for companies to conduct the retrospective analysis and ongoing monitoring that would be necessary to comply with the SEC's proposed material-in-the-aggregate reporting requirement.

Constantly reviewing previous minor incidents and frequently updating a living materiality assessment to incorporate new information on additional immaterial events would be extremely costly and burdensome—and would represent an inefficient use of company time and resources given the lack of benefit for investors. Further, there is no clear framework for determining whether immaterial events may be related, which would create further confusion and divert additional time and resources. Ultimately, companies do not have systems in place to regularly update a list of minor events and determine if or when they might rise to the level of materiality. The proposed reporting requirement for immaterial incidents is therefore likely to prove extremely difficult and costly for businesses despite its minimal utility for investors.

In addition to these practical considerations, disclosing as material a previously undisclosed series of immaterial events could introduce questions about inadequate disclosure practices—even though each incident was immaterial and the company made the appropriate decision in not disclosing it. The contradiction inherent in identifying a given incident as both immaterial and material could confuse investors and unnecessarily increase liability for businesses.

The NAM respectfully encourages the SEC to reconsider the proposed rule's provisions related to reporting on a series of immaterial cybersecurity incidents and instead to focus on ensuring the appropriate reporting framework for material breaches. The NAM opposes the proposed requirement, as conducting regular backward-looking materiality assessments about past minor incidents is not an efficient use of resources and will not provide useful information to investors seeking to understand a company's cybersecurity risks and practices.

[25] Proposed Rule, *supra* note 1, at 16619.

## V. The SEC should reconsider some of the proposed rule's more prescriptive risk management and governance disclosure requirements and instead adopt a more principles-based approach to cybersecurity risk reporting.

### A. Detailed public disclosures about a company's cybersecurity strategy and risk management could prove more useful to bad actors than to investors.

The proposed rule would require companies to disclose on an annual basis their policies and procedures related to cybersecurity strategy and risk management. Given the importance of strong cybersecurity protections in today's interconnected economy, the NAM supports substantive disclosure of the policies and procedures that companies have implemented to manage and mitigate cybersecurity risks—without providing a detailed playbook for potential hackers.

As such, the NAM appreciated that the SEC's 2018 guidance provided companies an outline for appropriate cybersecurity risk disclosure. Pursuant to the guidance, companies are already required to report material information on their cybersecurity risks (including the aspects of their business that give rise to such risks, the costs of maintaining appropriate cybersecurity protections, and steps taken to prevent or mitigate cybersecurity risks),[26] the effect of cybersecurity risks on their financial condition and their consolidated financial statements,[27] and any cybersecurity impacts on their products and services or relationships with customers and suppliers.[28]

The proposing release does not appropriately justify why more granular risk management and strategy disclosures are now necessary. The areas of focus in the proposed rule largely align with the 2018 guidance, but the rule would impose more prescriptive reporting requirements on public companies at every turn—without providing the requisite degree of flexibility needed to tailor the disclosures to a business's cybersecurity risk profile. It also would add significant burden and complexity given the increase in scrutiny and reporting obligations from other federal agencies since 2018. The NAM is concerned that the proposed risk management disclosures will not enhance cybersecurity, but rather will increase costs and confusion while also exposing potentially sensitive information to bad actors.

For example, the proposed risk management and strategy disclosures would require reporting on a company's cybersecurity risk assessment program, its activities to prevent and detect cybersecurity incidents, its cybersecurity contingency and recovery plans, and how previous incidents have informed any changes to its cybersecurity policies and procedures.[29] In 2018, the Commission made clear that a company need not "make detailed disclosures that could compromise its cybersecurity efforts—for example, by providing a 'roadmap' for those who seek to penetrate a company's security protections."[30] Yet the risk management disclosures included in the proposed rule could provide just such a roadmap. Manufacturers support appropriate descriptions of a company's cybersecurity risk management practices that are sufficient to inform shareholders about a business's risks and any efforts to mitigate them, but the SEC's detailed and prescriptive reporting requirements (especially the requirement to disclose how policy changes have been informed by previous incidents) could endanger rather than protect investors by making a company's "systems, networks, and devices more susceptible to a cybersecurity incident."[31]

---

[26] *See* 2018 Guidance, *supra* note 2, at 8169.

[27] *See id.* at 8170.

[28] *Ibid.*

[29] *See* Proposed Rule, *supra* note 1, at 16600.

[30] 2018 Guidance, *supra* note 2, at 8169.

[31] *Ibid.*

The NAM respectfully encourages the SEC to adopt a more principles-based approach to cybersecurity risk management and strategy disclosures. In 2018, the Commission made clear that it "expect[s] companies to disclose cybersecurity risks and incidents that are material to investors, including the concomitant financial, legal, or reputational consequences."[32] A disclosure framework based on this principle rather than line-item reporting mandates would better serve shareholders in the long run.

### B. The proposed requirement that public companies disclose the cybersecurity expertise of a specific board member could prove unnecessarily limiting.

The proposed rule would require companies to disclose their board and management cybersecurity governance and oversight practices. Companies would also be required to report on the cybersecurity expertise of company leadership.

In 2018, the SEC said that disclosures about the board's risk management processes should include the nature of the board's role in overseeing the management of material cybersecurity risks. The Commission also urged disclosure of "how the board of directors engages with management on cybersecurity."[33] To the extent that the proposed governance disclosure requirements align with the 2018 guidance on which companies already rely, the NAM supports appropriate reporting of both board and management oversight of cybersecurity risk. However, the NAM is concerned that the proposed requirement that public companies disclose the cybersecurity expertise of a specific board member could prove unnecessarily limiting.

As a matter of first course, the NAM does not believe that it is appropriate for the SEC to mandate specific criteria for candidates to public company boards of directors. Company boards are charged with broad strategy, governance, and risk management duties, and issuers and their shareholders are free to nominate and elect directors with a mix of diverse experience and expertise in order to meet these challenges. The SEC should not require the consideration or election of certain types of director candidates or impose disclosure requirements designed to achieve similar goals. Specific to cybersecurity, manufacturers know that effective cybersecurity governance does not require a single director with a certain technical degree, but rather an enterprise-wide focus on the issue and appropriate risk prioritization by the board. Effective risk management, including with respect to cybersecurity, falls under the purview of the entire board and management team, not just one director.

Further, the proposed rule's criteria for cybersecurity expertise are unnecessarily limiting and could discourage companies from considering otherwise qualified director candidates because their experience does not fit neatly under one of the SEC's proposed credentials. The qualifications necessary to manage cybersecurity risk in today's evolving threat landscape may not always align with the limited criteria in the proposed rule, and the rule's proposed qualifications could become more out-of-date as the threat landscape continues to evolve in the years to come. Further, the proposed rule focuses on specific technical expertise, job responsibilities, and professional certifications—yet the board of directors is charged with oversight and management of cybersecurity risk, not hands-on technology implementation and incident response. Expertise in these critical areas should also be prized by public companies looking for board leadership, not just specific technical skills.[34]

---

[32] *Ibid.*

[33] *Id.* at 8170.

[34] We would also note that diverting scarce talent away from operational jobs and toward board leadership could exacerbate companies' workforce challenges and ultimately hinder their ability to protect themselves from cybersecurity threats.

To the extent that the final rule maintains a disclosure requirement with respect to the board's cybersecurity expertise, the NAM respectfully encourages the SEC to broaden its proposed definition of "cybersecurity expertise" to include experience overseeing and managing cybersecurity risk. The NAM is hopeful that the final rule will not effectively mandate a certain board composition nor unnecessarily limit the diversity and experience of a company's board of directors.

* * * *

The NAM appreciates the SEC's continued attention to the importance of effective cybersecurity practices, governance, and risk management—and of appropriate disclosure of public companies' cybersecurity risks and incidents. The NAM believes that, with certain targeted changes, the SEC's proposed rule can support companies' efforts to provide material cybersecurity disclosures to their investors. A final rule that requires timely and accurate reports without instituting one-size-fits-all mandates will ensure that shareholders have access to useful information without exposing businesses, investors, and all Americans to increased risks. The NAM strongly supports a flexible approach to cybersecurity reporting, and manufacturers respectfully encourage the SEC to promulgate a final rule that allows public companies to both inform and protect their shareholders.

Sincerely,

Chris Netram
Managing Vice President, Tax and Domestic Economic Policy