ITI Promoting Innovation Worldwide

May 9, 2022

Re: ITI Comments on Securities and Exchange Commission Proposed Rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (RIN 3235-AM89; File Number S7-09-22)

The Information Technology Industry Council appreciates the opportunity to provide feedback to the Securities and Exchange Commission (SEC) on the Proposed Rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure. ITI is the premier global advocate for technology, representing the world's most innovative companies. Founded in 1916, ITI is an international trade association with a team of professionals on four continents. We promote public policies and industry standards that advance competition and innovation worldwide. Our diverse membership and expert staff provide policymakers the broadest perspective and thought leadership from technology, hardware, software, services, and related industries.

Cybersecurity and cybersecurity technology are critical to ITI members. Facilitating the protection of our customers (including governments, businesses, and consumers), securing, and protecting the privacy of individuals' data, and making our technology and innovations available to our customers to enable them to improve their businesses are core drivers for our companies. Consequently, ITI has been a leading voice in advocating effective approaches to cybersecurity, both domestically and globally. Cybersecurity is rightly a priority for governments and our industry, and we share the common goal of improving cybersecurity. Further, our members are global companies, doing business in countries around the world. Most service the global market via complex supply chains in which products are developed, made, and assembled in multiple countries around the world, servicing customers that typically span the full range of global industry sectors, such as banking and energy. We thus acutely understand the impact of governments' policies on security innovation and the need for U.S. policies to be compatible with – and drive – global norms, as well as the potential impacts on our customers.

As both producers and users of cybersecurity products and services, our members have extensive experience working with governments around the world on cybersecurity policy. In the technology industry, as well as banking, energy, and other global sectors, when discussing any cybersecurity policy, it is important to consider our connectedness, which is truly global and borderless.
ITI supports the SEC's intent to improve investors' awareness of material cybersecurity incidents and believe that in many instances offering information about cybersecurity incidents and governance procedures can help to improve transparency. However, we also have concerns with the way the proposed rule is currently written, including the fact that it could lead to disclosure of unmitigated vulnerabilities and that it may precede and thus overlap with the CISA rulemaking to implement the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA 2022). **As a result, ITI urges the SEC to delay implementation of the proposed rule to provide the SEC and stakeholders the opportunity to work through these challenges and allow the SEC the time to coordinate with the Cybersecurity and Infrastructure Security Agency (CISA) to deconflict the proposed rule with the forthcoming regulations to implement CIRCIA 2022.**

Below we offer perspectives on the proposed rule and respond to some of the specific questions posed. We structure our response to reflect 1) our overarching concerns related to the ways in

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

which this rule could serve to undermine cybersecurity, 2) our recommendation that the SEC delay implementation of the rule and work with CISA to streamline this measure with the implementation of the recently enacted CIRCIA 2022 to the extent possible, 3) our recommendation that the rule include safe harbor provisions for law enforcement, national security, and cybersecurity interests, 4) our view that the disclosure requirements undermine the relevance of "materiality", 5) our view that the four-business day post-materiality determination disclosure window may serve to undermine cybersecurity and will not achieve the SEC's objectives, 6) our recommendation that the SEC rule avoid requiring disclosure of incidents experienced by third-party vendors, and 7) our views on the other proposed disclosures, including related to cyber risk management and governance processes.

I. The SEC's proposed rule could result in the disclosure of Incidents prior to the mitigation of vulnerabilities, resulting in increased cybersecurity risks

In our view, which we believe is consistent with the Commission's intent, the resources and focus of incident reporting should first be on the technical realities of the incident response lifecycle from detection and analysis through recovery. ITI appreciates the proposed rule's statement that the Commission does not "expect a registrant to publicly disclose specific, technical information about its planned response to the incident or its cybersecurity systems, related networks and devices, or potential system vulnerabilities in such detail as would impede the registrant's response or remediation of the incident."[1] However, the rule also states in proposed Item 1.05, "a registrant shall make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident."[2] ITI believes a tension exists between these two positions as it introduces the likelihood that registrants would have to publicly disclose incidents prior to the mitigation of vulnerabilities.

Proposed Item 1.05, as well as the SEC's staff guidance back to 2011, fail to adequately take into account industry best practices and federal agency guidance on the handling of vulnerability disclosures.[3] As the federal government's own coordinated disclosure program makes clear, public disclosure of unmitigated vulnerabilities increases cybersecurity risks. The U.S. General Services Administration states, "we believe that disclosure [of vulnerabilities] in absence of a readily available patch tends to increase risk rather than reduce it, and so we request that you refrain from sharing your report with others while we work on our patch."[4] Similarly, the Cybersecurity and Infrastructure Security Agency (CISA) has established a 5-step process for coordinated vulnerability disclosure (CVD) the last of which is disclosure. CISA works with affected organizations to mitigate a vulnerability prior to disclosure.[5] Finally, a 2016 Research Report from the National

[1] SEC Proposed Rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, available at https://www.sec.gov/rules/proposed/2022/33-11038.pdf.
[2] SEC Proposed Rule, at 22.
[3] CISA DHS BOD 20-01, and ISO/IEC 30111 (2019), 29147 (2018), endorsed there, and also by Congress, see the IoT Cybersecurity Improvement Act.
[4] U.S. General Services Administration, Vulnerability Disclosure Policy (website last visited Apr. 30, 2022) available at https://www.gsa.gov/vulnerability-disclosure-policy.
[5] CISA Coordinated Vulnerability (CVD) Process (website lasted visited Apr. 30, 2022) available at https://www.cisa.gov/coordinated-vulnerability-disclosure-process#:~:text=CISA%20Coordinated%20Vulnerability%20Disclosure%20(CVD,the%20affected%20vendor(s).

Telecommunications and Information Administration (NTIA) found that "efforts to improve communication between researchers and vendors should encourage more coordinated, rather than straight-to-public disclosure."[6] The information communications and technology systems supply chain and ecosystem are deeply intertwined, making vulnerabilities and cyber threats potential risk factors for entities without association with one another. Indeed, requirements to disclose sensitive information concerning incidents, let alone vulnerability information, to the public at large stands in direct tension with existing federal guidance to maintain such information in confidence, and follow best practices and international standards for security and the handling of such information and incidents.[7] CIRCIA 2022 also provides that any vulnerability information, to the extent it is provided as part of an incident report, shall be protected and handled based on practices consistent with international standards and industry best practices for the handling and disclosure of such information.[8] These practices maintain that such information should be kept in strict confidence as its premature disclosure may enable attackers to harm end-users and the ecosystem at large.

While the SEC, as noted above, does not expect "technical information" to be disclosed, it is difficult to envision a public disclosure with the information described in Proposed Item 1.05 for Form 8-K without describing information about the exploited vulnerability. The Commission lays out five new elements for the 8-K disclosure including "a brief description of the nature and scope of the incident" and "the effect of the incident on the registrant's operations."[9] It will often be the case that registrants have to include information on specific technologies, vulnerabilities, or other technical information to explain the nature and scope of an incident or how that incident impacts registrants' operations. For instance, in the SolarWinds Corporation's December 17, 2020 (Commission File Number 001-38711) 8-K disclosure on their security incident describes vulnerabilities in its Orion monitoring products. Notably, SolarWinds Corporation's 8-K disclosure came after "hotfix updates to impacted customers" were released to "close the code vulnerability when implemented."[10]

As the SEC notes while discussing current disclosure practices of registrants, "it is foreseeable and perhaps even predictable that malicious actors will adapt their strategies and target companies in any industry where there are perceived vulnerabilities."[11] The public disclosure of unmitigated vulnerabilities will do just that, providing malicious actors with potentially valuable intelligence on which industries, companies, or vendors to target. We suggest that the Commission make it clear that the SEC will not require companies to submit Form 8-K disclosures until after the vulnerabilities at issue in a "material" incident have been mitigated.

Finally, we think it is important to highlight that in 2016 the Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system suffered an intrusion exposing non-public information to be filed on a

[6] Vulnerability Disclosure Attitudes and Actions: A Research Report from the NTIA Awareness and Adoption Group.
[7] See the IoT Cybersecurity Improvement Act and CIRCIA at 2245(a)(2)(E), as well as DHS CISA BOD 20-01.
[8] See H.R. 2471 § 2245 (a)(2)(B).
[9] SEC Proposed Rule, at 21.
[10] SolarWinds Corp. Form 8-K Report to the U.S. Securities and Exchange Commission on Dec. 17, 2020, Commission File No. 001-38711. available at https://www.sec.gov/Archives/edgar/data/1739942/000162828020017620/swi-20201217.htm.
[11] SEC Proposed Rule, at 17.

Form 8-K.[12] Chairman Clayton's testimony before the Committee on Financial Services on June 21, 2018 identified "deficiencies" in the Commissions "technical, process, and organization" which contributed to "internal delays in both the recognition of the intrusion itself and the internal appreciation of its scope and impact."[13]

II. The SEC should delay implementation of this proposed rule and work with CISA to ensure federal coordination to the extent possible

In light of the fact that the CIRCIA f2022 was signed into law in March 2022, adding to an already complex cyber incident reporting landscape, we encourage the SEC to strive to coordinate - and align and deconflict as appropriate - the incident disclosure components of this proposed rule with CIRCIA and other existing sectoral measures. Indeed, to the extent that critical infrastructure owners/operators are also publicly traded companies, they would fall within scope of both that law and this proposed rule, adding further complexity to an already saturated landscape for those companies. Rather than prematurely adding another layer of conflicting and overlapping incident reporting regulations that will necessarily draw legal and cyber incident response resources from the labor-intensive, fast-paced, and time-sensitive work of cyber incident response. We believe that it would be helpful for the SEC to first understand the direction that CISA is heading in with regard to the implementation of CIRCIA 2021, as understanding this context will help inform the direction the SEC takes in appropriately calibrating the proposed rule in a way that helps investors without harming cybersecurity.

To be clear, we are *not* recommending that the SEC mandate the disclosure of all technical details included in an incident report to CISA, as that information would not be useful to investors and the public release of that information could serve to further undermine cybersecurity. Indeed, this is one of the reasons that CIRCIA 2022 provides confidentiality and liability protections for entities that are required to report significant cyber incidents to CISA. Additionally, every significant incident reported to CISA will not be material. However, the SEC should work with CISA to see whether there is certain high-level information that overlaps between the two rules and whether reporting can be additionally streamlined to reduce the burden on companies that are subject to both rules. While we understand that the objectives of the SEC and CISA are different, we still believe it would be useful for the SEC to consider if and how to further streamline this disclosure requirement with that required by CIRCIA 2022.

As an example, the definition of "cyber incident" and "covered cyber incident" may differ, further causing divergence between the two measures. The proposed rule defines *cybersecurity incident* as an unauthorized occurrence on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein. Although aligned with the definition of "cyber incident" put forward in OMB M-17-12, the term 'jeopardizes' is concerning in this context, as many companies routinely have incidents that theoretically put data in jeopardy, but current reporting requirements generally require actual indications that data was lost and/or accessed. A mere vulnerability, without any evidence of exploitation, should not trigger disclosure requirements. As we reference above, not

[12] Testimony of Chairman Jay Clayton, SEC, before the Committee on Financial Services in a hearing entitled "Oversight of the U.S. Securities and Exchange Commission" on June 21, 2018. Available at https://www.sec.gov/news/testimony/testimony-oversight-us-securities-and-exchange-commission.
[13] Ibid.

everything that is reportable to CISA will be reportable to SEC, given the fact that if an incident is not material, it will not be and should not be reportable under the proposed SEC disclosure regime.

Beyond that, as CISA undertakes the rulemaking process to further define what constitutes a "covered cyber incident" for the purposes of the legislation, additional divergence may occur. To maintain consistency, then, we encourage the SEC to adopt the threshold definition of cyber incident as defined in CIRCIA 2022:

> *"(A) at a minimum, require the occurrence of—*
>
> *(i) a cyber incident that leads to substantial loss of confidentiality, integrity, or availability of such information system or network, or a serious impact on the safety and resiliency of operational systems and processes;*
>
> *(ii) a disruption of business or industrial operations, including due to a denial of service attack, ransomware attack, or exploitation of a zero day vulnerability, against*
>
> *(I) an information system or network; or*
>
> *(II) an operational technology system or process; or*
>
> *(iii) unauthorized access or disruption of business or industrial operations due to loss of service facilitated through, or caused by, a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider or by a supply chain compromise."*

We also encourage the SEC to proactively engage with CISA as the SEC seeks to implement this proposed rule. Under CIRCIA 2022, referenced above, CISA is tasked with leading an interagency council focused on streamlining incident reporting requirements. This is a mechanism that could prove useful in deconflicting potential requirements and ensuring that a disclosure requirement does not inadvertently undermine cybersecurity.

III. The SEC's proposed rule should include safe harbor provisions for law enforcement, national security, and cybersecurity interests

The SEC's rule will effectively pre-empt most state disclosure laws, many of which permit companies to delay data breach notices when law enforcement determines that such notices will impede an investigation. The SEC's proposed rules include no such exception, instead stating that "[o]n balance, it is our current view that the importance of timely disclosure of cybersecurity incidents for investors would justify not providing for a reporting delay."[14] We encourage the SEC to reconsider this position and amend the proposed rule to allow registrants to delay reporting of a cybersecurity incident when there is an active law enforcement investigation underway or when it is in the interest of national security. While states take varying approaches to providing for such exceptions, the language included in California's data breach law is illustrative: "The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation."[15]

[14] SEC Proposed Rule, at 25.

[15] See California Civil Code s. 1798.82, available here: https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.82

We also note that **question 7** of the proposed rule asks whether the rule should allow registrants to delay reporting a cyber incident where the Attorney General requests such a delay based on a written determination that the delay is in the interest of national security. As noted above, we support the inclusion of a safe harbor for a delay due to a national security interest. However, it is not clear how the structure proposed in the rule, where the Attorney General makes a written determination and requests a delay, would work in practice, particularly given it is uncertain whether sufficient information will be available to make such written determinations in a timely manner. This approach would have to be further contemplated, likely concurrently, by the DOJ in order for it to be implementable.

Relatedly, the Commission should consider a safe harbor where the public disclosure of the incident would jeopardize remediation of the incident. A public disclosure of a "material incident" to the SEC runs the risk of tipping off an adversary with multiple footholds on a target network. As indicated by CISA in a 2020 Joint Advisory, depending on the nature of the compromise and sophistication of the adversary the best practice may be to continue uncovering malicious activity to ensure the threat actor has been eradicated from the victim's network.[16] Additionally, as argued above, public disclosures of unmitigated vulnerabilities not only pose a cybersecurity risk to the registrant, but also to other users of the vulnerable technology. We also encourage the SEC to consider a safe harbor that allows registrants to delay disclosure where disclosure would, in good faith, jeopardize the remediation of a cyber incident or places other entities at risk, prior to the mitigation or patch of a vulnerability being available.

IV. The SEC's proposed cyber incident reporting requirements undermine the relevance of "materiality" and are unnecessary given its own substantial existing cybersecurity guidance

As the SEC notes in the proposed rule, the materiality principle has been a foundational element of the disclosure requirements in the federal securities laws since they were adopted in the 1930s and has been fleshed out in a series of Supreme Court cases including *TSC Industries, Inc. v. Northway, Inc.*, *Basic, Inc. v. Levinson*, and *Matrixx Initiatives, Inc. v. Siracusano.* Additionally, the SEC also points out that it has previously issued substantial interpretive guidance concerning the application of existing materiality-driven disclosure requirements under the federal securities laws to cybersecurity risks and incidents, most notably in 2011 and 2018.

However, the way the SEC proposes transforming that guidance into a set of new disclosure requirements related to cybersecurity incidents undermines the relevance of materiality in ways that will likely lead to the vast over-disclosure of cybersecurity incidents, potentially doing more harm than good to the cybersecurity of registrants and confusing investors, contrary to the SEC's intended purpose. While the SEC acknowledges in the proposed rule that materiality is an inherently subjective standard and that a materiality analysis is not a mechanical exercise, but rather must be driven by "consideration all relevant facts and circumstances surrounding the cybersecurity incident," several of the specific proposed incident reporting disclosure requirements

[16] Joint Advisory from the Cybersecurity and Infrastructure Security Agency entitled Technical Approaches to Uncovering and Remediating Malicious Activity (AA20-245A) originally released on Sept. 1, 2020. Available at https://www.cisa.gov/uscert/ncas/alerts/aa20-245a.

are inconsistent with this well-established approach and do not mesh well with the dynamic nature of cybersecurity incident response.

First, the proposed rule requiring the reporting of a series of previously immaterial cybersecurity incidents that, when analyzed retrospectively, have become material in the aggregate is unworkable. There are clearly many circumstances under which a "cybersecurity incident" would be immaterial to investors. The present cybersecurity reality as experienced by many large registrants is that they may experience hundreds or thousands of "cybersecurity incidents," as defined in the proposed rule, every day. Notably, under the recently passed federal incident reporting law, CIRCIA, the large majority of such incidents will not be defined as "significant" to be considered as covered incidents so as to trigger reporting requirements, a practical approach which serves the cybersecurity purpose of spurring the sharing cybersecurity incident information to improve operational collaboration and recognizes that companies should not be required to devote limited incident response resources to reporting insignificant incidents.

The SEC, however, has included a proposed requirement that registrants must "disclose a series of previously undisclosed individually **immaterial cybersecurity incidents** [that] has become material in the aggregate," an approach that will likely lead to over-disclosure of immaterial cybersecurity events, particularly amongst risk-averse registrants. The securities laws require disclosure of all risks that the company believes are material at the time of disclosure – considering both risk and probability – not risks that are presently immaterial but are potentially material at some unknown point in the future when combined with immaterial risks that have yet to occur. When coupled with the requirement that registrants report "any potential material future impacts," the aggregate reporting requirement creates just such an onerous, unbounded obligation continuous lookback over past immaterial incidents to draw inferences and relationships to determine aggregate materiality – requiring a level of public disclosure of cybersecurity incidents well beyond what is required to be confidentially disclosed to CISA under the new law. Rather than providing investors with useful information for informing investment decisions, the current approach, which provides open-ended lookback periods and no aggregation criteria, will inundate investors with precisely the "avalanche of trivial information" the Supreme Court sought to avoid in *Basic v. Levinson*.

We recommend that the proposed series/aggregate reporting requirement be eliminated entirely, or at a minimum, that the SEC include significantly more definitive guidance regarding how, under what circumstances, and over what period incidents are subject to this aggregation requirement

Second, the proposed rule requires the disclosure of details regarding "material" cybersecurity incidents irrespective of the materiality of those specific details. On its face, the proposed rule requires details to be disclosed about cyber incidents that are not material. For example, the proposed modifications to Form 8-k require the disclosure of detailed categories of information (e.g., "Whether any data was stolen or altered in connection with the incidents") irrespective of whether those details are themselves material. Whereas these types of details most certainly should be disclosed if they would be material to investors, there is no compelling rationale from a securities law standpoint or a cybersecurity standpoint for the SEC to include a prescriptive requirement that such details be disclosed in all cases. Further, because the nature of incident response is fast moving and ever evolving, companies are likely to over-disclose information before fully having their arms around what is relevant (and before being 100% sure of the information's accuracy) – so this set of requirements will also result in the disclosure of an "avalanche of trivial information."

We recommend, at a minimum, that the SEC clarify that any details it proposes to be disclosed regarding material incidents must also be individually qualified as "material." Otherwise, registrants will expend resources reporting immaterial details regarding incidents that are not relevant or helpful to investors.

Third, the proposed rule's ongoing reporting requirements would require ongoing analysis of present incidents, as well as potential future impacts of both "material" incidents and immaterial cyber incidents. Under the SEC's proposal registrants would need to devote resources to evaluating not only whether all cybersecurity incidents (including ongoing incidents) are "material" at present and "any **potential** material future impacts on the registrant's operations and financial condition," but also to continuously evaluate whether incidents previously determined to be immaterial may become material in the aggregate (as discussed above).

The inevitable result of these "ongoing review" requirements is that companies will spend significant resources analyzing *prior* cyber incidents, including those deemed not to be material at the time, to assess whether there needs to be an updated disclosure. Requiring registrants to disclose information irrespective of whether it is material to investors, thus resulting in information overload and obscuring material information, is contrary to the SEC's express rationale for the rule. We recommend that the SEC eliminate these onerous "ongoing" reporting requirements.

Finally, we believe the SEC does not provide a compelling justification for the rule. The proposed new incident disclosure requirements appear unnecessary, given the SEC in the proposed rule does not provide any compelling evidence that its existing guidance regarding cybersecurity disclosures is not currently being followed by registrants. Instead, the SEC offers as justification for the new proposed disclosure requirements anecdotal evidence that "staff has observed certain cybersecurity incidents that were reported in the media but that were not disclosed in a registrant's filings" and that the cybersecurity disclosures that were made "provide different levels of specificity" regarding various details, or that the cybersecurity disclosures varied by the size and type of company. Rather than serving as a justification for the prescriptive requirements in the proposed rule, this stated rationale suggests that the SEC's existing guidance **is working**, because each registrant should always be conducting an individualized, case-by-case analysis of whether a given cybersecurity incident it experiences is material – so it follows the disclosures, including the level of details and which companies are reporting them, should expectedly vary significantly.

V. The SEC's proposed "four business days" reporting timeline is unreasonable because it is likely to harm registrants' cybersecurity and unlikely to yield useful information to investors

The SEC sets forth one of the reasons for the "four business days" post-materiality determination timeline for its incident reporting requirement is to "significantly improve the timeliness of cybersecurity incident disclosures, as well as provide investors with more standardized and comparable disclosures." The SEC additionally cites as a rationale for the proposed rule "the growing concern that material cybersecurity incidents are underreported, and that existing reporting may not be sufficiently timely." It is telling that the SEC offers citations from CISA cybersecurity officials and others who were referring to the need for new federal cybersecurity reporting requirements (since passed in a new law, CIRCIA), which would require disclosure of

significant incidents to CISA – not the public disclosure of potentially insignificant cyber incidents and details. While improving the timeliness of cyber incident disclosures makes sense from a cybersecurity perspective and has been addressed by the passage of the new law, imposing a four-day post-materiality determination disclosure requirement that does not allow for any delay or other accommodation for cybersecurity purposes does not make sense from a cybersecurity perspective or the perspective of investors, for several reasons.

First, the four business days timeline proposed is unreasonable because a registrant can make a materiality determination and still be unlikely to have full, complete, and accurate information from the date of that determination. Requiring public disclosure within four business days of a materiality determination is too short of a timeline for imposing a blanket public disclosure requirement because in many cases a registrant will not have complete and accurate information necessary to make a disclosure useful (rather than misleading) to investors. Also, if a company must disclose early on in its investigation, the company's understanding of the incident may not be sufficiently nuanced and based on further investigation, the picture may change to be less severe, more severe, or just different, with varying degrees of negative cybersecurity impact. For example (1) the incident may look like it was caused by a certain type of attack (e.g., phishing) but further investigation may show credentials were stolen through a different attack method, (2) early on in an investigation, it may not be clear that something is important and/or sensitive so a company may disclose it based on a limited understanding, only to learn that the information is sensitive and should not have been disclosed once a fuller picture is established; (3) a threat actor could rapidly change their TTPs and pivot to a different attack vector/surface if information is disclosed on any remediation actions taken by the registrant; (4) an issuer might disclose that they have been subject to ransomware and/or made payment, and that information is later used by follow-on ransomware attackers to target victims for repeat attacks. In all the above circumstances, registrants or other dependent organizations could suffer significant harm if such disclosures are forced to be made public prematurely or before corresponding customer or dependent entity notifications can be made.

Second, a company may be able to determine that an incident is material at a stage when publicly reporting it would further compromise the company's security posture because it has not been adequately remediated. Not having exceptions for disclosures that reveal unremediated vulnerabilities would do more harm than good to investors because such disclosure may expose registrants to further incidents. Requiring disclosure of **unremeditated incidents within four days** would *not* enhance an investor's ability to evaluate the company's management of cyber risks, but is potentially disastrous from a cybersecurity standpoint, and likely to do more harm than good to the value of investors' investments in impacted registrants, because such disclosures may expose registrants to further incidents, compromise, or breach.

While the SEC says it "doesn't expect a registrant to disclose specific, technical information in such detail…that it would impede the registrant's response or remediation," inevitably requiring companies to file Form 8-K on accelerated timelines would result in the disclosure of sensitive security related technical information, possibly including information that jeopardizes national security. The contents of the disclosure would include a description of the nature and scope of the incident, as well as the incident's impact on the registrants' operations. Such disclosures could contain technically sensitive information on still unresolved vulnerabilities that could impact vendors or other users of that same vulnerable technology, potentially making the SEC disclosure a roadmap for other malicious actors. The uncertainty around the materiality standard, the

accelerated nature of the deadline and the potential liability attached to under-disclosing are additional exacerbating factors.

Ideally, as explored further in Section I of our paper, the SEC will modify the proposed disclosure requirements to clarify that information on unresolved vulnerabilities should be explicitly excluded from any public disclosures. At a minimum, the SEC should modify the rule to allow for a delay in reporting beyond four days to provide registrants with a reasonable opportunity to remediate active vulnerabilities.

Third, **as explored further in Section III, not allowing for exceptions to the four-day reporting requirement for active law enforcement investigations puts registrants further at risk without sufficient corresponding benefits to investors.** The information disclosed to the public on a "material incident" within four business days would not be "complete and accurate" information and could indeed be counterproductive if one of the goals is to improve cybersecurity practices amongst registrants. The SEC should provide an exception to the disclosure requirements during the pendency of an active law enforcement investigation into the incident, including to provide a safe harbor as discussed above.

VI. The SEC's proposed rule should not require the disclosure of incidents experienced by third-party technology vendors or service providers

The SEC highlighted companies' "increasing reliance on third party service providers for information technology services…" as one of the reasons cybersecurity risks have increased.[17] As with the proposed rule for investment advisers and companies, the SEC's proposed definition of information systems includes "information resources owned **or used by** the registrant…"In response to **question 10**, we encourage the SEC to consider the definition of "information systems" to include, "information resources *owned or controlled by* registrants." Such a limitation would more accurately capture a registrant's responsibilities over the cybersecurity incidents experienced on their systems and network. Alternatively, the SEC could include a safe harbor for information about cybersecurity incidents affecting information resources that are used but not owned by a registrant.

Registrants should only be required to disclose a cyber incident that happens on their own systems, not those of third-party vendors or service providers. This is the case for a number of reasons. First, in the event of a cybersecurity incident at a third-party vendor, public companies may have difficulty obtaining timely information to make a materiality determination for information systems they do not own or to provide sufficient details that would be required under the proposed rules. A third-party vendor's lack of responsiveness or slow response (both technically and in terms of information-sharing) could also put companies at risk of violating this regulation through no fault of their own. Information often trickles in slowly as the vendor's understanding of the incident evolves. Second, the third-party vendor or service provider challenge also raises security concerns, as laid out in greater detail above. Under the current language of the proposed rule registrants would be in a position to publicly disclose information on unmitigated vulnerabilities or active threats against other potential victims and/or their own customers. Third, a disclosure on third-party vendor or service provider incidents could also potentially run afoul of contractual obligations between the parties. As such, registrants should not be required to disclose unmitigated or ongoing

[17] SEC Proposed Rule, at 7.

cybersecurity incidents. Finally, data centers, which are registrants, should have a safe harbor from 8-K disclosure of cyber incidents which merely pass through their physical or virtual infrastructure and attack a data center tenant. We propose that where the attack does not target or impact the services the data center is providing (e.g., connection to the Internet backbone, power, cooling), only the tenant/target should be required to assess the materiality of an incident and make a disclosure under the proposed rule.

VII. While we believe several of the proposed disclosure requirements related to cyber risk management processes will help to improve investors' awareness, we also have concerns about the prescriptive nature of some of the disclosure requirements

ITI recognizes that cybersecurity is an important part of corporate governance and there is value to investors in receiving information about a company's cybersecurity risk management policies and procedures, their oversight of cybersecurity risks, and the board of directors' cybersecurity expertise. Requiring increased transparency around cybersecurity risk management practices is important for shareholders to make informed decisions about their investments. Shareholders should have access to information about which public companies are effectively addressing the risks of the negative impacts of cyber security breaches.

While we are generally supportive of the overarching disclosure requirements, we are concerned that the SEC's proposed governance disclosure is a very detailed, one-size-fits all approach, which implies best practices that might not make operational sense for companies. But, as a result of requiring this type of disclosure, it is inevitable that companies will devote resources to making performative changes to their cybersecurity governance to fit with these disclosures and those that do not will open themselves up to unnecessary liability. Indeed, one could envision a scenario where a company suffers a cybersecurity incident and then has to deal with a nuisance *Caremark* lawsuit based on whether it did or did not comply with these "best practices" as dictated by the SEC, an agency that is not best positioned to be determining or setting these standards. Further, we are also concerned that requiring the public disclosure of specific, detailed information relating to cyber risk management programs and processes could provide a roadmap to malicious cyber actors who could use such information to identify vulnerabilities in registrants' cyber defenses and tailor attacks accordingly.

Even so, we appreciate that there is benefit to disclosing certain information to investors. Below we offer additional responses to the SEC's questions to ensure the rule meets the SEC's intent to provide "decision-useful information" concerning "whether and how a registrant is managing cybersecurity risks [which] could impact an investor's return on investment" while avoiding requiring disclosures of details that could undermine the cybersecurity defenses of the registrant.[18]

Question 17 of the proposed rule asks whether the SEC should adopt Item 106(b) and (c) as proposed and whether there are other aspects of a registrant's cybersecurity policies and procedures or governance that should be required to be disclosed or excluded. ITI recommends that the SEC adopt (b)(i) and (b)(iv) of section 106(b) and (c), *with the changes referenced below*, and exclude proposed disclosures (b)(ii) b(iii), (b)(vi), b(vii), and b(viii), which we believe are too prescriptive and specific to disclose.

[18] SEC Proposed Rule, at 11.

- **Item 106(b)(iv):** We recommend merging sections (b)(iv) and (b)(v) into one disclosure that reads as follows: "The registrant undertakes activities to prevent, detect, minimize **[and/or respond to]** the effects of cybersecurity incidents."
    - We believe that both disclosures can be captured under one heading, as at a high-level this reflects the basic structure of a cyber risk management program. We encourage the disclosure here to remain high-level, allowing for flexibility in how companies choose to implement their cyber risk management programs.

Question 21 of the proposed rule asks whether a registrant should have to explicitly state that it has not established any cybersecurity policies or procedures.

- We believe a registrant should be required to explicitly state if they have not established any cybersecurity policies and procedures. Cybersecurity breaches can damage a company's financial condition and have indirect consequences to the overall health of the company as well. If an organization does not have adequate cybersecurity controls and defenses, shareholders have a right to know and factor in that risk to their investment decisions.

Question 22 of the proposed rule asks whether certain disclosures under Item 106 would have the potential to undermine a registrant's cybersecurity defense efforts or have other potentially adverse effects by highlighting a registrant's lack of policies and procedures related to cybersecurity.

- **Item 106(b)(vi):** We recommend **the deletion** of section 106(b)(vi): "Previous cybersecurity incidents informed changes in the registrant's governance, policies and procedures, or technologies."

Providing this information could disclose details about how registrants are protecting their enterprise and therefore undermine the cybersecurity defenses of the registrant. Such detailed disclosure could have the unintended result of making the registrant more vulnerable to cyberattacks. In addition, we oppose requiring registrants to disclose a cyber incident before it has been mitigated. Otherwise, cybercriminals could target the registrant and other companies and their affected customers, employees, or other constituents.

Question 23 of the proposed rule asks whether the SEC should exempt certain categories of registrants from proposed Item 106, such as smaller reporting companies, emerging growth companies, or FPIs and how any exemption would impact investor assessments and comparisons of the cybersecurity risks of registrants.

- We do not think the SEC should exempt any categories of registrants from proposed Item 106(b), including smaller reporting companies, emerging growth companies, or FPIs. All organizations are potential targets by threat actors, who typically cast a wide net and are indiscriminate in their threat activities. Further, it is often smaller organizations that have implemented the weakest cybersecurity defenses and are least mature in their basic cyber hygiene protections, such as regularly patching software, ensuring devices are properly configured, using multi-factor authentication, and enforcing least privileges to systems and

data. Increased transparency with respect to companies' cybersecurity risk management is valuable to investors when making investment decisions, regardless of filer type.

Question 24 asks whether the SEC should provide for delayed compliance or other transition provisions for proposed Item 106 for certain categories of registrants, such as smaller reporting companies, emerging growth companies, FPIs, or ABS issuers.

While we believe an overall delay in implementation of the SEC rule is warranted, we do not think the SEC should significantly delay compliance with Item 106 provisions based on the category of registrant, but instead provide for a period of transition for compliance. Cybersecurity risk assessment programs should be a foundational and strategic function of all organizations, no matter the age, size, or industry. A decision to delay compliance would signal that cybersecurity risk assessment is only relevant to specific segments of companies, when the reality is that all organizations are potential targets by threat actors. It is to the benefit of companies, their customers, and their shareholders to ensure that adequate cybersecurity controls and defenses are implemented without exception or the ability to skirt compliance due to a technicality.

Question 25-30 ask about disclosures related to the board of directors' cyber expertise. While we agree there is some value in informing investors about whether a registrant's board of directors has an oversight role regarding cybersecurity, including an oversight role regarding registrants' cybersecurity risk management practices, we have several concerns with this disclosure. We believe that such disclosures could serve to unnecessarily influence the composition of the board of directors, as publicly traded companies will try to fill board seats in order to align with the disclosure requirement to avoid "appearing that they do not take cybersecurity as seriously as other companies."[19] In this vein, we think it important to emphasize that there is currently a significant shortage of cybersecurity talent. While companies may want to fill seats with candidates' that have cyber expertise to align with the proposed disclosure requirements, there is unlikely a robust enough set of candidates that have cybersecurity expertise and are also qualified to hold a seat on the board of directors. So, it will be effectively impossible for all publicly traded companies to fill their board of directors with candidates that have cyber expertise. Additionally, larger public companies may be able to offer better incentives to those individuals with cyber expertise, putting smaller public companies at a disadvantage in terms of attracting and retaining those individuals.

In general, ITI believes that some of the disclosures specified in Item 106 regarding a registrant's policies and procedures for identifying and managing cybersecurity risks, a registrant's cybersecurity governance, including the board of directors' oversight role regarding cybersecurity risks, and management's role and relevant expertise in assessing and managing cybersecurity related risks and implementing related policies, procedures, and strategies would be beneficial in promoting transparency.

***

We appreciate the opportunity to share our perspective with the SEC. While we understand the objectives of the rule are to improve investor awareness of cybersecurity-related factors, we are concerned that it may in fact serve to undermine cybersecurity if not appropriately calibrated. We

[19] See Dissenting Statement of Commissioner Pierce here: https://www.sec.gov/news/statement/peirce-statement-cybersecurity-030922?utm_medium=email&utm_source=govdelivery

encourage the SEC to delay implementation of the proposed rule until CISA has further implemented its own rulemaking pursuant to CIRCIA 2021, so as to have a more fulsome understanding of the cyber incident reporting landscape. We are always happy to discuss our views further.