Before the Securities and Exchange Commission
Washington, D.C.

In the Matter of

Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure	)))	File No. S7–09–22

COMMENTS OF CTIA

Thomas C. Power
Senior Vice President and General Counsel

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

Melanie K. Tiano
Assistant Vice President, Cybersecurity and Privacy

CTIA
1400 16th Street, NW, Suite 600
Washington, DC 20036
[redacted]
www.ctia.org

May 9, 2022

Table of Contents

I. INTRODUCTION AND SUMMARY.

CTIA[1] welcomes the opportunity to comment on the Securities and Exchange Commission's ("SEC" or "Commission") proposed rules on cybersecurity risk management, strategy, governance, and incident disclosures ("NPRM").[2] CTIA provides comments to share concerns specific to the communications sector, which faces longstanding reporting obligations at the Federal Communications Commission ("FCC"), emergent incident reporting regulations from the Department of Homeland Security ("DHS"), and prior SEC regulation and guidance about cybersecurity. As the SEC considers potential rules in this area, we encourage the agency to consider the substantial overlap and compliance challenges that its proposal will create for companies in the communications sector.

As detailed below, the communications sector is on the front lines of cyber risk management, engaging in industry-based initiatives and working with government to promote secure communications networks and educate consumers about cyber risks. CTIA and its members provide innovative communications services that depend on trust in privacy and security. The sector was an early adopter of cyber best practices and partnerships, and industry proactively identifies, prevents, and remediates threats. CTIA's Cybersecurity Working Group ("CSWG") brings together all sectors of wireless—service providers, manufacturers, and wireless data, internet, and applications companies—to facilitate innovation and cooperation in

[1] CTIA® (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st-century connected life. The association's members include wireless carriers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry's voluntary best practices, hosts educational events that promote the wireless industry, and co-produces the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

[2] *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, Proposed Rule, 87 Fed. Reg. 16,590 (Mar. 23, 2022), https://www.govinfo.gov/content/pkg/FR-2022-03-23/pdf/2022-05480.pdf ("Proposed Rule").

response to evolving security threats. Through the CSWG, CTIA and its members engage in security policy discussions at the federal level and collaborate with federal partners, including the FCC, DHS, the National Institute of Standards and Technology ("NIST"), and the White House. CTIA's Privacy Working Group similarly brings together stakeholders to address data privacy. Additionally, CTIA has launched several initiatives that support secure wireless technologies.[3]

CTIA also participates in public-private partnerships that promote security across industry and government. These include:

- The Communications Information Sharing and Analysis Center, in which CTIA and its members partner with each other and government to share information, identify best practices, and address threats and incidents in real time.[4]
- The FCC's Communications Security, Reliability, and Interoperability Council, which "provide[s] recommendations to the FCC regarding ways the FCC can help to ensure security, reliability, and interoperability of communications systems."[5]
- DHS' Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force, which was spearheaded by CTIA and several member companies and addresses cyber threats to ICT supply chains through a "collective defense approach . . . bringing together industry and government to identify challenges and devise workable solutions."[6]

---

[3] For example, CTIA's Internet of Things ("IoT") Cybersecurity Certification Program establishes an industry baseline for device security on wireless networks and builds off of widely adopted cybersecurity standards from NIST and the International Organization for Standardization, among others. *See* Cybersecurity Certification Program for IoT Devices, Version 1.5, CTIA at 30 (Sept. 2021), *available at* https://ctiacertification.org/wp-content/uploads/2021/09/CTIA-Cybersecurity-Certification-Program-for-IoT-Devices-V-1-5.zip. Earlier this year CTIA launched a 5G Security Test Bed, a testing and validation initiative dedicated to commercial 5G networks. *CTIA Launches 5G Security Test Bed for Commercial 5G Networks*, PR Newswire (Jan. 12, 2022), https://www.prnewswire.com/news-releases/ctia-launches-5g-security-test-bed-for-commercial-5g-networks-301459627.html.

[4] *See Information Sharing and Awareness*, *Information Sharing and Analysis Centers (ISACs)*, CISA (last updated Feb. 16, 2022), https://www.cisa.gov/information-sharing-and-awareness.

[5] *Communications Security, Reliability, and Interoperability Council*, FCC, https://www fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-0 (last visited Apr. 23, 2022).

[6] *DHS And Private Sector Partners Establish Information And Communications Technology Supply Chain Risk Management Task Force*, CISA (last revised Feb. 5, 2021), https://www.cisa.gov/news/2018/10/30/dhs-and-private-sector-partners-establish-information-and-communications-technology.

CTIA and its members support transparency for market participants. Public communications companies make appropriate disclosures about governance and incidents, consistent with SEC guidance and informed by SEC enforcement priorities. They participate in robust Environmental, Social, and Corporate Governance efforts. Aspects of their cyber practices are overseen by state and federal agencies, from the FCC, Federal Trade Commission ("FTC"), and SEC to the New York State Department of Financial Services and other regulators.

Drawing from experience defending customers and their networks, managing compliance programs, and as targets of malicious cyber attacks, CTIA and its members urge the SEC to reconsider its proposed cybersecurity disclosure rules. In particular, the incident disclosure mandate as proposed is likely to generate confusion in the marketplace, increase cyber risk to regulated companies, and have other unintended consequences, given that the proposed timeline is very short with little flexibility. The proposed mandate will also overlap and may conflict with comprehensive regulatory efforts being undertaken at the direction of Congress, and should be reviewed to permit harmonization and deconfliction. Additionally, the SEC should reconsider its proposed governance rules, which do not account for the varied needs of companies in diverse industries. CTIA therefore respectfully urges the SEC to reconsider the proposed rules, or in the alternative, modify them to promote harmonization with existing regimes and reduce the risk of premature disclosures that could undermine investigations and lead to market confusion.

II. THE WIRELESS INDUSTRY IS A LEADER IN CYBERSECURITY AND ALREADY PROVIDES IMPORTANT INFORMATION ON CYBERSECURITY RISK AND INCIDENTS.

Companies in the wireless industry prioritize provision of cybersecurity risk and incident information to customers and the public, sharing information under existing legal regimes and on their own accord to promote customer trust and safety. The wireless industry is also regulated by the FCC, in several relevant respects. Wireless carriers are subject to the FCC's rules requiring

agency, law enforcement, and customer notification after unauthorized access to customer proprietary network information ("CPNI").[7] In addition to FCC requirements, wireless carriers comply with disclosure obligations under state law, which may require notices to individual consumers and state regulators.[8] Providers are also subject to FCC reporting requirements regarding network outages.[9]

The SEC premises its new rule proposal on the belief that "investors would benefit from more timely and consistent disclosure about material cybersecurity incidents" and companies' "cybersecurity risk management, strategy, and governance practices."[10] Public wireless carriers make robust disclosures about cyber incidents and forward-looking risk management in SEC filings. These issues are front of mind for the wireless industry, which aims to educate consumers about cyber risk, assure the public of the security of networks—which is an imperative in the competitive wireless market—and communicate information about cyber events when they occur. These disclosures are robust; a Moody's report cited by the SEC found that telecommunications and media companies, along with banks, "had the most thorough disclosures" in SEC filings on cybersecurity.[11] The public may also learn about cyber incidents in the wireless industry through news reporting, information issued by impacted organizations, and state Attorneys General.[12]

---

[7] 47 C.F.R. § 64.2011.

[8] *See, e.g.*, N.Y. Gen. Bus. Law § 899-aa(2) (requiring notice to individuals); Cal. Civ. Code § 1798.82(f) (requiring notice to state Attorney General).

[9] 47 C.F.R. § 4.9.

[10] Proposed Rule at 16,593.

[11] *Research Announcement: Cybersecurity disclosures vary greatly in high-risk industries*, Moody's Investors Service (Oct. 3, 2019), https://www.moodys.com/research/Moodys-Cybersecurity-disclosures-vary-greatly-in-high-risk-industries--PBC_1196854; Proposed Rule at n.34.

[12] *E.g.*, *Data Security Breaches*, Delaware Department of Justice, https://attorneygeneral.delaware.gov/fraud/cpu/securitybreachnotification/ (last visited Apr. 18, 2022); *Maryland Information Security Breach Notices*, Maryland Attorney General,

Beyond disclosing incidents, CTIA and its members take seriously the need to inform and educate the public on how carriers address cyber risk and how customers can protect themselves. CTIA publishes consumer resources on protecting networks and devices.[13] AT&T provides resources to help customers understand cyber risk and safeguard their sensitive data, as well as a yearly report on cybersecurity trends.[14] Verizon issues a yearly Data Breach Investigations Report to help organizations protect themselves from security threats.[15] T-Mobile educates consumers on online safety and identity theft protection, and compiles resources for consumers impacted by online fraud.[16] These and other resources provide timely and consistent public information about cybersecurity risks and threats and the wireless industry's risk management and cybersecurity governance practices, making additional requirements unnecessary.

III. THE SEC SHOULD RECONSIDER ITS PROPOSED INCIDENT DISCLOSURE RULES, WHICH ARE NOT NECESSARY IN LIGHT OF EXISTING INCIDENT REPORTING REQUIREMENTS AND NEW RULES BEING CREATED AT THE DIRECTION OF CONGRESS.

A. The SEC's Current Regime Promotes Transparency on Cyber Incidents, Making New Disclosure Rules Unnecessary.

The SEC's current reporting regime appears to be sufficient to achieve the goals outlined in the NPRM. As the SEC acknowledges in the NPRM,[17] the SEC has issued multiple guidance documents in recent years making clear the disclosure obligations of public companies with

---

https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/breachnotices.aspx (last visited Apr. 18, 2022).

[13] *Protecting Your Data*, CTIA, https://www.ctia.org/protecting-your-data.

[14] *Privacy Center*, AT&T, https://about.att.com/privacy html; *AT&T Cybersecurity Insights™ Report: Securing the Edge*, AT&T, https://cybersecurity.att.com/resource-center/industry-reports/cybersecurity-insights-report-eleventh-edition.

[15] *Data Breach Investigations Report 2021*, Verizon, https://www.verizon.com/business/resources/reports/dbir/.

[16] *Privacy Center: Resources for identity theft and internet fraud prevention.*, T-Mobile, https://www.t-mobile.com/privacy-center/education-and-resources/online-safety.

[17] Proposed Rule at 16,593.

respect to cybersecurity incidents.[18] Pursuant to this guidance, companies routinely make disclosures after a material incident. Under its current rules, the SEC is empowered to police the adequacy of disclosures. Indeed, it frequently engages in investigations and has pursued related enforcement actions.[19]

B. The SEC's Proposed Disclosure Regime Would Add Complexity to an Already Fragmented Landscape.

The current incident reporting landscape for companies is fragmented and complex. There are multiple incident reporting and notification requirements that publicly traded companies comply with—at both the state and federal level. To begin with, all 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have breach notification laws.[20] These laws require notice directly to consumers, and in many cases, to state regulators.[21] At the federal level, several requirements exist, and more are emerging. This creates complexity and compliance challenges. For example, a telecommunications sector company that has experienced a cyber incident may need to:

- Notify federal law enforcement of the breach under the FCC's CPNI rules;
- Notify affected individuals of the breach under the FCC's CPNI rules;
- Identify and comply with reporting obligations under county, state, and state public utility commission notification rules;
- Analyze whether the incident triggered overseas reporting obligations;

---

[18] CF Disclosure Guidance: Topic No. 2, SEC (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2 htm; *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, Interpretation, 83 Fed. Reg. 8166 (Feb. 26, 2018), https://www.govinfo.gov/content/pkg/FR-2018-02-26/pdf/2018-03858.pdf ("SEC 2018 Guidance").

[19] *See, e.g.*, SEC, Press Release, *SEC Announces Enforcement Results for FY 2021* (Nov. 18, 2021) (stating agency pursued 697 enforcement actions in fiscal year 2021).

[20] *See Security Breach Notification Laws*, National Conference of State Legislatures (Jan. 17, 2021), https://www ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

[21] *Id*.

- If the incident disables the company's communications network for at least 30 minutes, make initial and final reports regarding the outage to the FCC;[22] and
- If the company is a government contractor and the incident affects a covered information system or defense information, report the incident to the DoD.[23]

All of these obligations may be layered on top of the company's own efforts to address and mitigate the breach, work with federal security agencies and local law enforcement, and inform the public of the issue. The SEC's proposal threatens to further complicate these efforts.

Additional obligations may also be forthcoming. The FCC is currently considering updates to its CPNI breach notification requirements, which may add additional obligations.[24] The FTC has proposed to amend its Standards for Safeguarding Customer Information to require that covered financial institutions report to the FTC certain security events.[25] Further, President Biden recently signed into law the Cyber Incident Reporting for Critical Infrastructure Act ("CIRCIA"), which imposes new reporting obligations on public companies owning and operating critical infrastructure across sixteen sectors.[26] Examples of varying federal approaches are illustrated in the Appendix in Table 1, *Federal Regimes*, and Table 2, *Examples of State Regimes*, describes the contours of state law requirements.

Given existing and forthcoming reporting requirements, the SEC should consider how it can harmonize its work with existing and emerging reporting requirements, which already apply

---

[22] *See* 47 C.F.R. Part 4.

[23] DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.

[24] *Chairwoman Rosenworcel Circulates New Data Breach Reporting Requirements*, FCC (Jan. 12, 2022), https://www.fcc.gov/document/chair-rosenworcel-circulates-new-data-breach-reporting-requirements.

[25] *Standards for Safeguarding Customer Information*, Supplemental notice of proposed rulemaking; request for public comment, 86 Fed. Reg. 70,062 (Dec. 9, 2021), https://www.govinfo.gov/content/pkg/FR-2021-12-09/pdf/2021-25064.pdf.

[26] Consolidated Appropriations Act, 2022, Pub. L. 117-103, Div. Y ("CIRCIA").

to many of the public companies that the SEC aims to regulate here. Indeed, it is not clear how establishing another reporting regime would benefit the public. New disclosure obligations would provide little value in light of the various other public sources of information and disclosure regimes. Further, in the critical days following an attack, company personnel already must navigate myriad existing regimes and deadlines, which can divert resources from cyber response and remediation. Before moving forward, the SEC should carefully consider whether further reporting is necessary and, if so, craft a regime more consistent with existing federal policy.

C. The SEC Should Take a Risk-Based Approach and Prioritize Confidentiality and Care in Disclosure.

1. *Existing Consensus Approaches to Cyber Policy Take Risk-Based Approaches, Including One Recently Directed by Congress.*

Congress, DHS, and other agencies have championed a risk-based policy approach to addressing cyber incidents. Fundamentally, the SEC should take care to avoid taking cyber policy in a new and different direction for such a large swath of the U.S. economy, particularly as DHS embarks on its rulemaking to establish a reporting regime that prioritizes confidentiality and care in sharing information to advance national and homeland security.

First, the SEC should recognize differences among sectors and home in on risk. The SEC's proposal would apply to all publicly traded companies and does not appear to grapple with differences in industries, company sizes, or risk profile.[27] By contrast, other cyber regulatory approaches embrace targeted and flexible approaches. For example, the Transportation Security Administration's ("TSA") interim Security Directives are targeted at a subset of regulated industries and purport to respond to particular threats.[28] The forthcoming

[27] *See* Proposed Rule at 16,593.

[28] Security Directive 1580-21-01, Enhancing Rail Cybersecurity, TSA(December 31, 2021),

DHS rules under CIRCIA will apply to entities in sixteen critical infrastructure sectors[29] and DHS can tailor rules to higher-risk events and contexts. NIST's seminal cybersecurity guidance document, the *Framework for Improving Critical Infrastructure Cybersecurity*, as well as other best practices, acknowledge the importance of flexibility.[30] The SEC proposal does not appear to reflect a risk-based approach to the sort of varied entities, incidents, and impacts that should trigger mandatory disclosures.

Second, the SEC should not depart from other regimes that build in flexibility in the timeline for disclosure. Flexibility may be necessary to account for the time necessary to investigate and fully evaluate the consequences of an incident. To this end, California, for example, requires disclosure in "the most expedient time possible and without unreasonable delay."[31] Further, regimes requiring public disclosures provide for delay while victims work with law enforcement, in order to protect the integrity of investigations.[32] Notably, the FCC *prohibits* customer and public notification until a carrier "has completed the process of notifying law enforcement" and "7 full business days have passed after [such] notification."[33] The various, significant reasons to establish a more flexible reporting period are detailed in Section IV. The SEC should conform its approach to this well-recognized principle.

---

https://www.tsa.gov/sites/default/files/sd-1580-21-01_signed.pdf (freight rail); Security Directive 1582-21-01, Enhancing Public Transportation and Passenger Railroad Cybersecurity, TSA (Dec. 31, 2021), https://www.tsa.gov/sites/default/files/sd-1582-21-01_signed.pdf (passenger rail and rail transit).

[29] *Critical Infrastructure Sectors*, CISA (last updated Oct. 21, 2020), https://www.cisa.gov/critical-infrastructure-sectors.

[30] Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, NIST, at vi (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[31] Cal. Civ. Code § 1798.29(a).

[32] 47 C.F.R. § 64.2011(b)(1); N.J. Stat. Ann. § 56:8-163(c)(2).

[33] 47 C.F.R. §§ 64.2011(a), (b)(1).

Third, the SEC regime should reflect the policy goals of confidentiality and care in disclosure of information, which are hallmarks of existing regimes and the bipartisan CIRCIA just recently signed into law. As shown in Appendix Table 1, the TSA, DHS, and DoD regimes encourage confidential reporting of sensitive information. Moreover, as DHS implements CIRCIA, it will build upon the extensive privacy and civil liberty protections for information shared provided in the legislation.[34] Information shared voluntarily under the Cybersecurity Incident Sharing Act of 2015 ("CISA 2015"), and information that will be required to be reported under CIRCIA, is shared for cybersecurity purposes within the federal government.[35] Further, information shared with state and local governments and other companies for cybersecurity purposes is anonymized and not attributable to the victim company. The SEC's proposal is a departure from this approach in that all disclosed information will be public. While the SEC is attempting to advance the goal of investor awareness, by placing this goal ahead of the consensus approach in other regulations, the SEC risks undermining the confidentiality and intelligence-gathering that characterize existing reporting.

2. *New Requirements That Overlap, Duplicate, or Conflict with Existing Regimes Undermine Government Efforts at Harmonization.*

The SEC's proposal comes as Congress and the executive branch are engaged in concerted work to expand and harmonize incident reporting. CIRCIA reflects Congress's intent to minimize duplicative reporting requirements, as it directs the establishment of a Cyber Incident Reporting Counsel to "coordinate, deconflict, and harmonize Federal incident reporting

[34] 6 U.S.C. § 1504(b); Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015, DHS and DOJ (Jan. 4, 2021), https://www.cisa.gov/sites/default/files/publications/CISA_PCL_Guidelines_Periodic_Review_2020_final.pdf.

[35] 6 U.S.C. §1504; CIRCIA § 2245.

requirements, including those issued through regulations."[36] Additionally, at the first meeting of the FCC's relaunched Cybersecurity Forum for Independent and Executive Branch Regulators, convening officials representing 30 regulatory and advisory agencies,[37] Chairwoman Rosenworcel remarked that the group should focus on "achieving greater consistency in the reporting of cyber incidents. Right now, there's a lot of fragmentation across sectors and jurisdictions in what information gets reported, when and how it is reported, and how that information can be used. So we'll discuss using this Forum as a place to work toward greater convergence on these matters."[38] These ongoing federal harmonization initiatives heighten the need for the SEC to reconsider this proposal, as it would only add to an already heavily fragmented reporting landscape.

IV. IF THE SEC MOVES FORWARD WITH ITS PROPOSAL, IT SHOULD BUILD FLEXIBILITY INTO ITS RULES, WHICH WOULD BETTER ACCOMMODATE THE NEEDS OF COMPANIES, VICTIMS, LAW ENFORCEMENT, AND THE PUBLIC.

A. The SEC's Proposed Four-Business Day Timeline May Not Enable Companies to Provide Accurate Information That Meets the SEC's Goals.

The SEC proposes to require registrants to disclose information about a material cybersecurity incident "within four business days after the registrant determines that it has experienced a material cybersecurity incident."[39] However, as shown in Appendix Tables 1 and 2, a four-business day timeline does not align with other cyber reporting regimes that affected

[36] CIRCIA § 2246(a).

[37] *Chairwoman Rosenworcel to Lead Relaunched Federal Interagency Cybersecurity Forum*, FCC (Feb. 3, 2022), https://docs.fcc.gov/public/attachments/DOC-379926A1.pdf.

[38] *Remarks of Chairwoman Jessica Rosenworcel to the Cybersecurity Forum of Independent and Executive Branch Regulators*, FCC (Apr. 8, 2022), https://docs fcc.gov/public/attachments/DOC-382215A1.pdf.

[39] Proposed Rule at 16,595.

registrants may be subject to, and the SEC does not provide any particularized justification for this timeline, as compared with other regulatory regimes or in terms of public benefits.

This short timeline is ill-suited for cyber incident disclosures. Investigations into even relatively straightforward cyber incidents can be lengthy, and a material incident may require months of analysis before a victim can confidently address the types of information that the SEC would have them make public within four days. As NIST has explained:

> When an event of interest has been identified, analysts assess, extract, and analyze [various] data with the goal of determining what has happened and how the organizations systems and networks have been affected. This process might be as simple as reviewing a few log entries on a single data source and determining that the event was a false alarm, or as complex as sequentially examining and analyzing dozens of sources (most of which might contain no relevant data), manually correlating data among several sources, then analyzing the collective data to determine the probable intent and significance of the event. However, even the relatively simple case of validating a few log entries can be surprisingly involved and time-consuming.[40]

The SEC should be careful to consider the diversity of attacks and the realities of investigations and avoid an unduly short timeline for cyber incident reporting. Cyber investigations and containment can take weeks or months; they also evolve over time as facts develop.[41] As DHS has observed, forensic analysis may be a part of incident management but may be managed by different personnel, who may be reliant on the incident response team and their activities.[42] A short disclosure period may rush forensic analysis, which in the ordinary

---

[40] NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response Recommendations of the National Institute of Standards and Technology, NIST, at 6-11 (Aug. 2006), https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-86.pdf.

[41] IBM, Cost of a Data Breach Report 2021, IBM, at 22 (2021), https://www.ibm.com/downloads/cas/OJDVQGRY (reporting that in 2021 it took an average of 212 days to identify, and an average 75 days to contain a breach). Verizon's Data Breach Incident Report looked at "more than 79,000 breaches in 88 countries—showed approximately 60% of incidents were discovered within days. However, 20% could take months or more before organizations realized something was amiss." Shane Schick, *Data breach detection time: How to minimize your mean time to detect a breach*, Verizon (2021), https://www.verizon.com/business/resources/articles/s/how-to-minimize-your-mean-time-to-detect-a-breach/.

[42] *See e.g.,* Recommended Practice: Creating Cyber Forensics Plans for Control Systems, DHS, at 40 (Aug. 2008), ("The forensics function inside an organization can be designed to support the incident response function, both

course may flow from incident containment and remediation work. Assuming that under such timelines a materiality determination is made between discovery and full containment, a four-business day disclosure period may run before containment, and well before reliable forensic analysis is complete.

While the SEC emphasizes the need for timely incident information, its focus on speed overlooks the possibility that rushed disclosure will lead to less accurate or relevant incident information.[43] The SEC proposes to mandate disclosure of:

- when the incident was discovered and if it is ongoing;
- a brief description of nature and scope;
- whether any data was stolen, altered, accessed, or used for unauthorized purpose;
- effect of incident on registrant operations;
- whether incident is remediated or being remediated.[44]

It is quite possible that four business days after an incident's materiality has been determined, some or all of this information will be uncertain, preliminary, or in flux because a company's assessment of the nature, extent, and impact of an incident is likely to evolve as forensic and other investigations develop information.

As a result of these complexities, disclosure within four business days of a materiality determination may result in premature or erroneous facts being disseminated to the public, causing harm to consumers, shareholders, and company goodwill.[45] Some commentators have

---

during and after initial response phases.") https://www hsdl.org/?view&did=7971.

[43] *See, e.g.*, Proposed Rule at 16,595.

[44] *Id*. at 16,624.

[45] *See, e.g.*, *Taking a Customer-Centric Approach to a Data Breach: Insights from Crisis Response*, Deloitte, at 12, https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-Data-Breach-Customer-Centric-POV-EN-AODA.pdf (noting that "timely notification without the proper level of detail can actually amplify customer frustration" and lead to litigation) (last visited Apr. 23, 2022); Tanner De Witt, *Data Breach Response: The Management Response*, Tanner De Witt Solicitors (Feb. 10, 2021), https://www.tannerdewitt.com/management-data-breach-response/ ("Accuracy is critically important. The trust of customers and stakeholders will be challenged if a series of notices serves to highlight contradictions or misleading information. . . . Any benefit from prompt notice will be lost if that notice was misleading and did not give stakeholders the information they needed to respond

cautioned about organizations rushing through important forensics investigations to meet regulatory deadlines,[46] which hinders their ability to fully recover from a security incident. A rushed disclosure timeline also increases burdens on victim organizations, who will be managing technical response, recovery, and remediation, as well as multiple possible reporting obligations. In the days and weeks after a cyber incident occurs or is identified, companies should not be compelled to divert resources from critical tasks like remediation to resolving conflicts among various compliance requirements and deadlines.

The SEC's proposed timeline appears to be based on its reporting timeframe for other types of occurrences, but it is inappropriate for cyber events. The SEC requires disclosure on a company's Form 8-K within four business days of certain triggering events.[47] While four days may be workable for clearly ascertainable events, such as the date of completion of an acquisition or disposition of assets, an amendment to the registrant's articles of incorporation, or the departure of a director or officer, the SEC should not apply this strict timeline to a determination that a material cyber incident has occurred. In these other contexts, there is no uncertainty as to the matter being disclosed, and no risk of premature disclosure. The differences between cyber events—perpetrated by malicious actors of dubious identity, which can require months of analysis—and the sorts of developments now subject to a four-day notice period show that such a short period is not appropriate for cyber incidents.

---

appropriately.").

[46] *See Cost of a Breach: Forensics and Notification*, Protenus (Sept. 14, 2016), https://www.protenus.com/resources/cost-of-a-breach-forensics-and-notification.

[47] *See* Form 8-K, Section B, SEC, https://www.sec.gov/files/form8-k.pdf.

B. A Four-Business Day Timeline Would Make It More Difficult for Law Enforcement and National Security Agencies to Work with Victims, Take Protective Measures, and Try to Identify Perpetrators.

There are several reasons to proceed cautiously with making public disclosures about cybersecurity incidents. It is critical that corporate victims of cyber attacks not release information that could impede law enforcement investigations—and in light of this reality, many federal and state regimes allow for delayed disclosures to facilitate ongoing investigations. At a minimum, the SEC should reconsider its proposed timeline and look carefully at options to enable responsible disclosures that do not jeopardize law enforcement work, that minimize risk to victim companies and consumers, and that do not flood the securities markets with low-quality information that may be more misleading than helpful.

When and how to make public disclosures is an important facet of cyber incident response. Security agencies such as the FBI and victim companies "will generally coordinate public statements concerning the incident with victim companies to ensure that harmful or sensitive information is not needlessly disclosed. Victim companies should likewise consider sharing press releases regarding a cyber incident with investigators before issuing them to avoid releasing information that might impede the ongoing investigation."[48] An inflexible SEC reporting mandate could thwart such strategic information release.

Government-industry collaboration, including a coordinated approach to disclosure of sensitive information, can help generate positive outcomes after an attack. The SEC should aim to promote this type of collaboration. The federal government has been working to encourage companies to partner with the Federal Bureau of Investigations ("FBI") and DHS to report

[48] *Best Practices for Victim Response and Reporting of Cyber Incidents Version 2.0*, DOJ, at 19 (Sept. 2018), https://www.justice.gov/criminal-ccips/file/1096971/download.

incidents to help identify and take action against malicious actors.[49] Indeed, the government has touted cooperation to increase the chance to recover data and funds.[50] Discreet cooperation can also be vital to develop mitigations for systemic vulnerabilities. This hard work and trust-building has proven valuable. For example, after Colonial Pipeline fell victim to a ransomware attack, the company cooperated with an FBI-led investigation, resulting in recovery of millions in cryptocurrency.[51]

The FBI recognizes the sensitivity and value of collaboration. As a senior FBI official noted about a recent success: "Thanks to information shared with us by a member of private industry, the FBI executed an innovative court-authorized operation to copy and remove those backdoors from hundreds of vulnerable computers across the country."[52] This successful federal-private sector coordination respected the need for care and confidentiality in handling sensitive cyber information, as the FBI explained: "Maybe most importantly to the private sector, we only did this after publicly releasing information on the compromises and working with Microsoft to directly contact server owners to allow them time to fix the problem on their own."[53] These types of coordination and collaboration must continue and the SEC should be careful to not impede these efforts.

---

[49] Cyber Incident Reporting: A Unified Message for Reporting to the Federal Government, DHS, https://www.dhs.gov/sites/default/files/publications/Cyber%20Incident%20Reporting%20United%20Message.pdf (last visited Apr. 22, 2022).

[50] *See id*.

[51] Evan Perez, et al., *First on CNN: US recovers millions in cryptocurrency paid to Colonial Pipeline ransomware hackers*, CNN (June 8, 2021), https://www.cnn.com/2021/06/07/politics/colonial-pipeline-ransomware-recovered/index.html.

[52] *Oversight of the FBI Cyber Division, Hearing Before the H. Comm. on Judiciary*, 117th Cong. 5 (2022) (statement of Bryan A. Vorndran, Assistant Director, Cyber Division, FBI), https://docs.house.gov/meetings/JU/JU00/20220329/114533/HHRG-117-JU00-Wstate-VorndranB-20220329.pdf.

[53] *Id*.

C. The Proposed Timeline Could Expose Victims to Greater Cybersecurity Threats and Re-Victimization.

Another risk of the SEC proposal is that it could open the door to additional attacks for a company and its customers that have already been victims of cybercrime. One reason that federal law enforcement pursues an approach centered on confidentiality and discretion[54] is that disclosures about cybersecurity incidents can be a valuable source of information for bad actors. For example, detailed disclosures can undermine the company's efforts and expose them as a target for additional attacks. In its 2018 guidance, the SEC was correct to note that "[t]his guidance is not intended to suggest that a company should 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. We do not expect companies to publicly disclose specific, technical information about their cybersecurity systems, the related networks and devices, or potential system vulnerabilities in such detail as would make such systems, networks, and devices more susceptible to a cybersecurity incident."[55] This approach was sound, as disclosure of incidents and associated details could give bad actors a roadmap to exploit systems.

Additionally, premature disclosures may encourage bad actors to exploit and re-victimize companies and their customers. Re-victimization of companies after a cybersecurity incident is a real threat, and publicly confirming a breach or releasing information about incidents serves as an invitation to malicious actors and opportunists. For example, there have been copycat attempts and anonymous personas on the dark web that claim to have copies of exfiltrated data or

---

[54] *See Small Business Information Sharing: Combating Foreign Cyber Threats*, FBI (Jan. 30, 2018) (testimony from Cyber Division Deputy Assistant Director Howard Marshall before the House Small Business Committee), https://www.fbi.gov/news/testimony/small-business-information-sharing-combating-foreign-cyber-threats. "[t]he FBI's approach in working with potential or actual victims of cyber intrusions or attacks is to first and foremost, and to the best of our ability, use our processes to protect the victim from being re-victimized, and to provide confidentiality and discretion during the investigative process."

[55] SEC 2018 Guidance at 8,169.

information, piling burdens onto victim companies to evaluate claims and determine how to respond.[56] Further, it is not uncommon to see customers whose data has been involved in a breach be preyed on by fraudsters. For example, bad actors may attempt to reach out to customers pretending to offer assistance or remediation post-breach.[57] These kinds of practices already occur, but publicizing incidents early in a uniform manner would encourage them.

For these reasons, state and federal laws recognize the benefits of careful and properly timed disclosures[58] and companies in the midst of a cyber incident are careful about disclosures. As NIST has noted in guidance on cyber information sharing, "unauthorized disclosure of information" about cyber incidents "may impede or disrupt an ongoing investigation, jeopardize information needed for future legal proceedings, or disrupt response actions such as botnet takedown operations."[59] The concept of responsible public disclosure is familiar to security professionals, as in the context of vulnerabilities, where the government and the private sector recognize the need to balance the potential benefits of providing information to the public against risks involved with premature disclosure.[60] As the European Telecommunications Standards Institute explains in its *Guide to Coordinated Vulnerability Disclosure*, premature public disclosures can reduce security by informing malicious actors before protections are in place.[61]

---

[56] *See, e.g.*, Mathew J. Schwartz, *'SolarLeaks' Site Claims to Offer Attacks Victims' Data*, BankInfo Security (Jan. 13, 2021), https://www.bankinfosecurity.com/solarleaks-site-offers-supply-chain-attack-victims-data-a-15751 (discussing online group's claims of selling data stolen from entities that were victims of the SolarWinds breach despite no hard evidence to support the claims).

[57] *FBI Issues Warning after Extortion Schemes Surface Following Spate of Mega Breaches*, Trendmicro (June 3, 2016), https://www.trendmicro.com/vinfo/fr/security/news/cyber-attacks/fbi-warning-after-extortion-schemes-surface-following-mega-breaches

[58] *See* Colo. Rev. Stat. § 6-1-716(2)(a); 47 CFR § 64.2011(b).

[59] NIST Special Publication 800-150, Guide to Cyber Threat Information Sharing, NIST, at 4 (Oct. 2016), http://dx.doi.org/10.6028/NIST.SP.800-150.

[60] *See e.g.,* Draft NIST Special Publication 800-216, NIST, at 16 (June 2021), https://doi.org/10.6028/NIST.SP.800-216-draft.

[61] ETSI TR 103 838 V1.1.1, Cyber Security; Guide to Coordinated Vulnerability Disclosure, ETSI, at 8 (Jan. 2022),

So too with many cyber incidents, where containment or remediations may not be in place within four days. The SEC should reconsider aspects of its proposal that may result in these unintended consequences.

V. IF INCIDENT REPORTING RULES ARE ADOPTED, THEY SHOULD BE WORKABLE FOR REGISTRANTS, PROMOTE COLLABORATION WITH LAW ENFORCEMENT, AND PROVIDE THE TIME NECESSARY TO DISCLOSE ACCURATE AND USEFUL INFORMATION.

If the SEC proceeds with incident reporting rules for public companies, CTIA urges the SEC to reconsider several elements and amend its proposal.

A. Any SEC Disclosure Requirement Should Prioritize Provision of Accurate Information Over Speed by Permitting Flexibility in the Timing of Disclosures.

If the SEC proceeds with an incident disclosure mandate, it should ensure that any timeline for disclosure be greater than four business days after determination that a material incident occurred and account for the flexibility needed in dealing with a cyber incident. Consistent with these principles, the SEC should consider requiring reporting "without unreasonable delay." This type of standard for a reporting timeframe is particularly appropriate for public disclosures, where accuracy and reliability should be prioritized over speed. In other contexts, Congress has directed 72-hour reporting to CISA under CIRCIA because of the expectation that the agency may be able to provide operational support to respond and remediate and may benefit from rapid situational awareness of cyber threats for intelligence and homeland security purposes. But the SEC has no such operational need for speed, so the utility of a four-business day disclosure period for investor decision making is unclear, and such a short period

https://www.etsi.org/deliver/etsi_tr/103800_103899/103838/01.01.01_60/tr_103838v010101p.pdf.

may lead to the disclosure of incomplete or premature information, which could mislead the public and investors.

B. Any Adopted Rules Should Permit Delayed Reporting for National Security or Law Enforcement Purposes.

The SEC should reconsider its conclusion that its new mandate "would not provide for a reporting delay when there is an ongoing internal or external investigation related to the cybersecurity incident."[62] The SEC should allow registrants to delay reporting, for these and other national security or law enforcement reasons, including ongoing investigation of the culprit, cause, and extent of security incidents. As shown in Appendix Table 2, several state laws provide that a company may delay notification if law enforcement determines notice may impede a criminal investigation.[63] Notably, the FCC's CPNI disclosure rules *prohibit* carriers from disclosing a breach to the public until seven business days have passed after notification to the Secret Service and the FBI.[64] Any SEC rules should account for such permissible delays.

Accommodating law enforcement needs is consistent with the SEC's approach in other areas. For example, the SEC Enforcement Manual provides that, "in certain circumstances it is appropriate for criminal authorities to ask SEC staff to refrain from taking actions that would harm the criminal investigations."[65] The rule should also "allow registrants to delay reporting of a cybersecurity incident where the Attorney General requests such a delay based on the Attorney General's written determination that the delay is in the interest of national security," as the SEC

---

[62] Proposed Rule at 16,596.

[63] *E.g.*, Cal. Civ. Code § 1798.82(c); N.J. Stat. Ann. § 56:8-163(c)(2); N.Y. Gen. Bus. Law § 899-aa(4).

[64] 47 CFR § 64.2011.

[65] Enforcement Manual, SEC, Division of Enforcement, Office of Chief Counsel, at 85 (Nov. 28, 2017), https://www.sec.gov/divisions/enforce/enforcementmanual.pdf.

asks in the NPRM.[66] Any SEC cyber disclosure requirements must properly account for the well-established needs of law enforcement with respect to cybercrime investigations.

C. The SEC Should Avoid Creating Ongoing Reporting Requirements Without a Deadline.

The SEC should reconsider its proposal to require a registrant to provide "updated disclosure in periodic reports about previously reported cybersecurity incidents,"[67] as this could transform a one-time incident disclosure into a never-ending requirement for ongoing disclosures about shifts of any magnitude in the registrant's policies and procedures. Companies often update their regulators and consumers about developments in a major cyber incident, making additional mandates from the SEC superfluous while creating an ongoing compliance burden for reporting companies.

The SEC's proposal is broad and would require information about "any" changes in policies and procedures as a result of the cyber incident at any point in the future, not just material changes or changes that occurred in a certain timeframe.[68] This open-ended, perpetual requirement would add to the burden registrants already face in disclosing material information in their periodic filings. Additionally, the requirement would not provide a corresponding benefit to market participants, who can obtain much of the same information—filtered through a materiality lens—in a more digestible format through the registrant's typical SEC filings.

---

[66] Proposed Rule at 16,598.

[67] *Id*. at 16,593.

[68] *Id*.

D. The SEC Should Refrain from Adopting Overly Broad Definitions and Triggers, Which May Create Internal Compliance Challenges and Lead Companies to Overreport.

If the SEC proceeds with an incident disclosure mandate, it should narrow its definitions and triggers. A broad new disclosure obligation, as proposed in the NPRM, will complicate compliance in several important ways. For example, public companies maintain programs to monitor and prevent insider trading and have adjusted their approaches to address material cybersecurity events and risks. Some programs include robust internal and external monitoring and are often tailored to particular incidents and the personnel involved, which can vary over time based on complexity and severity of an incident. Compliance functions will become particularly complex considering the SEC's consideration of repeated minor incidents becoming material in the aggregate or over time,[69] which could mean that routine information about daily cyber activities becomes insider information. If disclosure and reporting obligations expand without clear guidance, companies may—in an abundance of caution—need to presumptively treat entire security departments and functions as possessing potential inside information and further restrict trading, disadvantaging those employees.

Overly broad or undefined obligations may also lead to unhelpful reporting of incidents that are not truly material, which may confuse or mislead investors. Broad or unclear reporting requirements could lead thousands of publicly traded companies to report incidents as often as daily. In particular, the SEC should reconsider its proposed requirement that registrants must update incident disclosures "when a series of previously undisclosed individually immaterial cybersecurity incidents has become material in the aggregate."[70] It will be extraordinarily

[69] *Id*.

[70] *Id*. at 16,599.

challenging for a company to determine when several potentially unrelated incidents may "become material."[71]

Sweeping, vague requirements could put companies in the difficult position of reporting every potential incident or facing penalties. At the same time, the SEC should not place itself as the arbiter of determining whether a material critical incident occurred. The nature and criticality of cyber incidents will vary across industries and companies, making one-size-fits-all rules or guidance inapt. The SEC must eschew an overly broad, all-encompassing approach.

E. Any Rule Should Incorporate Safe Harbors and Protections for Companies Reporting Incidents in Good Faith.

Companies required to comply with an SEC incident reporting regime should have a safe harbor from enforcement if they delay reporting due to a determination by the company or law enforcement that disclosure would impede the investigation and resolution. As the SEC proposes, it would be appropriate to amend Rules 13a-11(c) and 15d-11(c) under the Securities Exchange Act of 1934 ("Exchange Act") to include new Item 1.05 in the list of Form 8-K items eligible for a limited safe harbor from liability under Section 10(b) or Rule 10b-5 under the Exchange Act.[72] Additionally, companies reporting pursuant to the new rules should have a safe harbor from liability for properly disclosed forward-looking claims.[73]

These safe harbor protections are necessary due to the substantial litigation risks and burdens companies will face. Securities class action litigation can be abused and should be reserved for cases that truly harm investors and shareholders. To ensure any incident reporting

[71] *Id*.

[72] *Id*. at 16,597.

[73] *See* 15 U.S.C. § 77z-2 (providing safe harbor for forward-looking statements).

rules do not lead to unjustified litigation over good-faith judgment calls relating to ongoing or past security incidents, the SEC should include appropriate safe harbors.

VI. THE SEC SHOULD RECONSIDER ITS PROPOSED GOVERNANCE DISCLOSURE RULES.

A. Companies Are Best Positioned to Determine the Ideal Makeup of Boards.

The SEC proposes to require public companies to disclose the cyber expertise of the members of the board of directors,[74] with the apparent goal of encouraging companies to select board members with cybersecurity backgrounds or experience. This requirement should not be adopted. The criteria outlined by the SEC in determining whether a board member has "cybersecurity expertise"[75] does not reflect the range of experiences, beyond cybersecurity backgrounds or credentials, that could contribute to robust board oversight of cyber risk management. Board members may have varied experiences that contribute to oversight of a company's cyber risk, such as having managed organizations through cyber response in the past.

Companies are in the best position to determine the ideal makeup and size of their boards. When seeking board members, expertise in specific areas may be useful, but diversity of background, experience, and skills are primary concerns.[76] Companies and their advisors factor in a broad range of considerations when determining the appropriate composition of their boards. The boards of AT&T, Verizon, and T-Mobile, for example, are composed of a diverse set of individuals with varied background and experience,[77] which fosters robust company oversight

---

[74] *See* Proposed Rule at16,600.

[75] Proposed Rule at 16.602.

[76] *See, e.g.*, Jeffrey A. Sonnenfeld, *What Makes Great Boards Great*, Harvard Business Review (Sept. 2002), https://hbr.org/2002/09/what-makes-great-boards-great

[77] *See, e.g.* Corey Anthony, *We Hear You, Loud and Clear*, AT&T (July 14, 2021), https://about.att.com/inside_connections_blog/2021/diversity_equity_inclusion_annual_report.html (discussing diversity of Board of Directors); *Diversity and Inclusion*, Verizon, https://www.verizon.com/about/our-company/diversity-and-inclusion; Jeff Green, *T-Mobile Leads Boardroom Diversity Gains for S&P 500 Companies*, Bloomberg (July 15, 2021), https://www.bloomberg.com/news/articles/2021-07-15/t-mobile-push-for-board-

and protection of shareholder interests. Studies have found that governance and shareholder interests can be best promoted through "recruiting demographically diverse directors who also help improve cognitive diversity in the boardroom."[78] Companies pursue various goals in building diverse and innovative boards; these efforts, which benefit investors, should not be limited or disfavored by additional expectations for specialized expertise that may be not be plentiful across the economy.[79]

The SEC's proposal would potentially hinder companies' ability to establish a board with the optimal skills and experience to protect investor interests by encouraging them to choose members who have a specific set of cybersecurity credentials, rather than other relevant experience or alignment with other corporate priorities and obligations. Certain registrants, such as those doing classified work for the U.S. government, may need to address national security experience in determining the makeup of their boards. Others may want to focus on geopolitical issues or supply chain. The Commission's proposal could crowd out other areas of expertise and harm companies that provide critical services to the U.S. government. Smaller or resource-constrained companies may face challenges in hiring board members that have the specific cyber expertise the Commission would require and be put at a disadvantage in the market.

---

diversity-leads-june-gain-in-s-p-500 (a "wide range of experience and perspective, as well as diversity in gender, race and ethnicity, absolutely makes us a better organization," CEO Mike Sievert said in an emailed statement).

[78] Jared Landaw, *Maximizing the Benefits of Board Diversity: Lessons Learned From Activist Investing*, Harvard Law School Forum on Corporate Governance (July 14, 2020), https://corpgov.law.harvard.edu/2020/07/14/maximizing-the-benefits-of-board-diversity-lessons-learned-from-activist-insting/.

[79] Cybersecurity expertise is in short supply across the economy, *see, e.g.,* NIST NICE, https://www.nist.gov/document/workforcedemandonepager2021finalpdf and GAO, GAO-19-144, *Cybersecurity Workforce* (2019) ("the federal government and private industry face a persistent shortage of cybersecurity and IT professionals to implement and oversee information security protections to combat cyber threats."). Within the cyber work force, observers have found that "[m]inority professionals make up a significant portion of the cybersecurity workforce, but are underrepresented across senior roles within their organizations." (ISC)^2 Global Information Security Workforce Study at 8 (2018) available at https://www.isc2.org/Research/Cybersecurity-Diversity#.

Mandated disclosures may serve little purpose, as cyber risk management may not necessarily be a responsibility of an individual board member. Companies use various tools for cyber risk management, including board committees, audit committees, and other specially tasked groups to address risks to their operations. Part of good governance includes relying on appropriate subject matter experts, both within a company and through outside consulting engagements, to inform management.[80] Further, a mandate is not needed to raise awareness of the importance of cybersecurity issues in governance. Scholarly and industry work shows that cyber is on the radar for senior executives and boards,[81] who address cyber risk and other emerging issues in various ways along with other priorities like diversity, innovation, turnover, optimal composition, and roles.[82]

Moreover, it is also unclear how an investor would productively use information about a board member's expertise. Investors may not themselves have cybersecurity backgrounds or know how to assess a board members' cybersecurity credentials. It is unrealistic to assume that investors will find information regarding the cyber credentials of an individual on the board useful in informing their investment decisions.

There are also questions about the legality of such a requirement. While couched in the context of a disclosure requirement, this proposed rule would serve as an implicit direction from

---

[80] *See Resource Center*, NACD, https://www.nacdonline.org/insights/resource_center.cfm?itemnumber=20789 (providing resources such as board assessment of effectiveness of cybersecurity programs, tools for directors in building relationships with the chief information security officer and broader cybersecurity team).

[81] *See* Scott Chase, *Directors to Watch 2021 Rank Top Issues for Public Company Boards*, Directors & Boards, https://www.directorsandboards.com/articles/singledirectors-watch-2021-rank-top-issues-public-company-boards (discussing results of survey identifying top issues and priorities for boards, with threat of ransomware and cybersecurity breaches taking third spot).

[82] *See, e.g.,* George M. Anderson & David Chun, *How Much Board Turnover Is Best?*, Harvard Business Review (Apr.2014), https://hbr.org/2014/04/how-much-board-turnover-is-best; David F. Larcher & Brain Tayan, *Board Composition, Quality, & Turnover*, Stanford Business School (April 2020), https://www.gsb.stanford.edu/faculty-research/publications/cgri-research-spotlight-board-composition-quality-turnover.

the SEC to public companies on how they should conduct their cybersecurity programs. While Congress authorized the SEC to regulate corporate governance under the Sarbanes-Oxley Act's disclosure requirement related to audit committee financial experts,[83] here the SEC proposes to go several steps further by requiring disclosure of the subject matter expertise of board members that have a wide range of responsibilities that go beyond cybersecurity. Such requirements should be adopted only to the extent mandated by federal legislation.

B. The SEC Should Not Require Disclosures on Registrants' Risk Management, Strategy, and Governance.

Disclosures on cyber risk management and strategy may offer bad actors insight into a company's strategy and allow them to identify vulnerabilities more easily. The FBI has advised that malicious actors look at SEC filings and key events to target victims.[84] Malicious efforts could increase if bad actors can find cyber risk management, key personnel, and changes to strategy, in SEC filings.

Cybersecurity is a nuanced, multi-faceted concept that affects public companies in vastly different ways across sectors. The SEC should not impose its judgment of what proper cyber risk management should look like by requiring registrants to make specific disclosures on cyber policies and governance. There is no one-size-fits-all approach to cybersecurity. Companies need flexibility to address cybersecurity threats in a manner that best fits the unique circumstances that they confront. Mandating specific governance requirements for cybersecurity would limit this important flexibility and hamstring companies into rigid governance structures that could hinder their broader risk management efforts.

---

[83] 15 U.S.C.§ 7265.

[84] *See* FBI PIN 20211101-001, Private Industry Notification: Ransomware Actors Use Significant Financial Events and Stock Valuation to Facilitate Targeting and Extortion of Victims, FBI, (Nov. 01, 2021), https://www.cisa.gov/sites/default/files/publications/PIN_202111101.pdf.

Further, new rules are unnecessary when existing rules and guidance already direct companies to disclose these types of information where relevant. The SEC's rules already require a company to "disclose the extent of the board's role in the risk oversight of the registrant, such as how the board administers its oversight function, and the effect that this has on the board's leadership structure."[85] Also, the SEC's 2018 Guidance noted that "[t]o the extent cybersecurity risks are material to a company's business, we believe this discussion should include the nature of the board's role in overseeing the management of that risk."[86] The information that is currently provided is sufficient to inform market participants on this topic.

VII. CONCLUSION

CTIA appreciates this opportunity to comment and encourages the SEC to reconsider, or in the alternative, modify the proposed cyber incident and risk management disclosure rules. CTIA recommends the SEC align any new rules with other federal requirements and reporting regimes and ensure that, in encouraging provision of accurate information to market participants, it does not invite negative, unintended consequences.

Respectfully submitted,

/s/ Melanie K. Tiano
Melanie K. Tiano
Assistant Vice President, Cybersecurity and Privacy

Thomas C. Power
Senior Vice President and General Counsel

Thomas K. Sawanobori
Senior Vice President, Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

[85] 17 CFR § 229.407(h); 17 CFR § 240.14a-7.

[86] SEC 2018 Guidance at 8170.

CTIA
1400 16th Street, NW, Suite 600
Washington, DC 20036
202-736-3200

May 9, 2022

APPENDIX TABLES

Table 1 – Federal Cyber Incident Reporting Regimes

Authority or Agency	Who Must Report?	What Triggers an Obligation to Report?	To Whom? [Public or Confidential Basis?]	Report Timeframe	May Law Enforcement Delay Victim and Public Notification?
SEC – Proposed Rule[87]	**All** public companies	A "material cybersecurity incident." Materiality is based on the existing standard, which may include the nature, extent, or potential magnitude of an incident, and harm to company's reputation, financial performance, customer and vendor relationships, and litigation or regulatory risk.	File with SEC (Form 8-K, 6-K, and 20-F) [PUBLIC REPORT]	Within **4 business days** of determination of a material cybersecurity incident; materiality determination must be made "as soon as reasonably practical"; update report in 10-Q or 10-K.	X
FCC[88]	**Only** telecommunications carriers.	Breach of customers' proprietary network information.	Secret Service and FBI [CONFIDENTIAL REPORT]	Within **7 business days.**	✓ For up to 30 days, and may extend as needed.
TSA[89]	**Only** freight and passenger railroad	Cybersecurity incidents on IT or OT systems including:	DHS CISA	Within **24 hours of identifying** the	N/A- no public report.

[87] *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, Proposed Rule, 87 Fed. Reg. 16590 (Mar. 23, 2022), https://www.federalregister.gov/documents/2022/03/23/2022-05480/cybersecurity-risk-management-strategy-governance-and-incident-disclosure.

[88] 47 C.F.R. § 64.2011.

[89] Security Directive 1580-21-01, Enhancing Rail Cybersecurity, TSA(December 31, 2021), https://www.tsa.gov/sites/default/files/sd-1580-21-01_signed.pdf (freight rail); Security Directive 1582-21-01, Enhancing Public Transportation and Passenger Railroad Cybersecurity, TSA (Dec. 31, 2021), https://www.tsa.gov/sites/default/files/sd-1582-21-01_signed.pdf (passenger rail and rail transit); *Ratification of Security Directive*, Notification of ratification of directive, 86 Fed. Reg. 38,209 (July 20, 2021); *see also* TSA IC Pipeline-2022-01, Enhancing Pipeline Cybersecurity,

	carriers, rail transit operators, and pipeline owner/operators; Directive effective for one year due to active threat environment.	- unauthorized access - malware - denial of service Any other cyber incident that results in operational disruption, or has the potential to impact large numbers of customers, critical functions, or public health/ national security.	[CONFIDENTIAL REPORT] Report is not public and shared only for cybersecurity purposes; non-Federal entities receive anonymized threat indicators and defensive measures; reporting is liability-shielded and may not be used for regulatory enforcement.	cybersecurity incident. Recognizes additional information may become available	
DHS[90]	**Only** entities in one of the 16 critical infrastructure sectors; rulemaking will further define based on risk factors.	Reportable incidents include: - Substantial loss of confidentiality, integrity, or availability of a system or network - Serious impact on operational systems and processes - Disruption of business or industrial operations	DHS CISA [CONFIDENTIAL REPORT] Report is not public and shared only for cybersecurity purposes; non-Federal entities receive anonymized threat indicators and defensive measures; reporting is liability-shielded and may not be used for regulatory enforcement.	Within **72 hours of covered incident** Recognizes "substantial new or different information" may become available Notify CISA when incident "has concluded and been fully mitigated and resolved."	N/A- no public report.
DHS[91]	**Only** entities in one of the 16 critical infrastructure sectors experiencing a ransomware attack.	A ransom payment for a ransomware attack.	DHS CISA [CONFIDENTIAL REPORT] Report is not public and shared only for cybersecurity purposes; non-Federal entities receive anonymized threat indicators and defensive measures; reporting is liability-	Within **24 hours of ransom payment** Must file new report if ransomware incident becomes "substantial," even if already reported ransom payment.	N/A- no public report.

https://www.tsa.gov/sites/default/files/TSA%20Information%20Circular%20Pipeline-2022-01%20Package.pdf (pipeline owners and operators).

[90] Pub. L. 117-103, Sec. 2242. Rule is not yet in effect.

[91] Pub. L. 117-103, Sec. 2242. Rule is not yet in effect.

			shielded and may not be used for regulatory enforcement.		
DoD[92]	**Only** federal contractors supporting DoD	Discovery of a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract.	DOD [CONFIDENTIAL REPORT] DoD may conduct a forensic analysis or share information obtained from contractor with government entities that conduct counterintelligence or law enforcement investigations.	Within **72 hours** of discovery of a cyber incident.	N/A- no public report.

[92] DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.

Table 2 – Examples of State Data Breach Reporting Regimes

State	Who Must Report?	What Triggers an Obligation to Report?	To Whom?	Report Timeframe	May Law Enforcement Delay Victim and Public Notification?
California[93]	Person or company doing business in California that owns or licenses computerized data that includes personal information.	Unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or encrypted personal information if the key or security credential also acquired.	**Victims:** Notify affected California residents, and if more than 500 California residents affected must notify the California Attorney General.	"In the most expedient time possible and without unreasonable delay."	✓ if a law enforcement agency determines that the notification will impede a criminal investigation.
Colorado[94]	Company or public entity that collects personal information for business purposes.	Unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information.	**Victims:** Notify affected Colorado residents, and if more than 500 Colorado residents affected must notify the Colorado Attorney General.	Within **30 days.**	✓ consistent with law enforcement needs or incident response.
New Jersey[95]	Companies doing business in New Jersey or public entities that collect personal information.	Unauthorized access to electronic files, media or data that compromises the security, confidentiality or integrity of personal information.	**Victims and Law Enforcement:** Notify NJ State Police, then affected residents.	"Without unreasonable delay."	✓ if a law enforcement agency determines that the notification will impede a criminal or civil investigation.

[93] Cal. Civ. Code § 1798.82.

[94] Colo. Rev. Stat. § 6-1-716.

[95] N.J. Stat. Ann. § 56:8-163.