May 9, 2022

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

RE: File No. S7-09-22; RIN 3235-AM89: SEC Proposed Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

Dear Ms. Countryman,

The Securities Industry and Financial Markets Association ("SIFMA")[1] welcomes the opportunity to respond to the proposed rule issued by the Securities and Exchange Commission (the "Commission" or "SEC") on March 9, 2022. The proposed rule concerns "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure" with respect to public companies subject to the reporting requirements of the Securities Exchange Act of 1934 (the "Proposal").[2] The Commission further requested comments on best practices with respect to such cybersecurity disclosures.

SIFMA acknowledges the unquestioned importance of cybersecurity to our country and economy, and to all public companies[3] and their investors.[4] Accordingly, we applaud the Commission for its continuing attention to corporate cybersecurity risk management. However,

[1] SIFMA is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets. On behalf of our industry's one million employees, we advocate on legislation, regulation and business policy affecting retail and institutional investors, equity and fixed income markets and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA). For more information, visit http://www.sifma.org.

[2] *See* Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release Nos. 33-11038; 34-94382; RIN 3235-AM89 (proposed Mar. 9, 2022) (the "Proposal").

[3] Please note that references here to "public companies" or registrants concern companies that are subject to the reporting requirements of the Securities Exchange Act of 1934.

[4] *See* Cybersecurity Resources, SIFMA, *available at* https://www.sifma.org/resources/cybersecurity-resources/; *SIFMA Statement on Completion of Quantum Dawn VI Cybersecurity Exercise*, SIFMA (Nov. 18, 2021), *available at* https://www.sifma.org/resources/news/sifma-statement-on-completion-of-quantum-dawn-vi-cybersecurity-exercise/; *see also* Kevin Eiden *et al.*, *Organizational cyber maturity: A survey of industries*, MCKINSEY & COMPANY (Aug. 4, 2021), *available at* https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/organizational-cyber-maturity-a-survey-of-industries (finding that banking and healthcare the sectors with the best overall cybersecurity-management profiles and that more profitable companies build stronger cybersecurity capabilities).

the Commission should distinguish between its role as prudential[5] regulator for regulated entities versus its role to assure that public filings under the Exchange Act meaningfully inform investors regarding their investment decisions. As the Proposal stands now, we respectfully submit that the SEC is calling for public disclosure of considerably too much, too sensitive, highly subjective information, at premature points in time, without requisite deference to the prudential regulators of public companies or relevant cybersecurity specialist agencies (like the Cybersecurity and Infrastructure Security Agency ("CISA")). Essentially, such disclosures would benefit cyber attackers more than they would investors. Moreover, the Proposal could be improved by taking into account public companies' need to conduct essential internal cybersecurity investigations, coordinate with law enforcement, intelligence and national security agencies, and comply with court orders that may restrict the timing of permissible cybersecurity disclosures.

CISA Director Jen Easterly's recently said that CISA is not in the business of "stabbing the wounded."[6] The SEC's present Proposal, in contrast, would do just that by denying a registrant proper time and focus to remediate and mitigate the impacts of an incident. Further, the Proposal blocks the company's ability to collaborate responsibly with other U.S. agencies (and their foreign counterparts). It also exposes investors to premature, excessive, risky and potentially misleading disclosures. The Proposal strikes the wrong balance by forcing companies to report to the SEC and shareholders prematurely – i.e., before they have an opportunity to collaborate fully with relevant government agencies, and implement effective remediation, mitigation and disruption of the relevant cyber risk. In other words, the Proposal's conclusion 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 [for law enforcement investigations]"[7] is seriously misguided. The U.S. Government has repeatedly invoked the essential importance of public-private collaboration to defend against serious cyber-attacks,[8] but the SEC's Proposal ignores what makes such partnerships work. We respectfully submit that relevant U.S. (and international) cybersecurity agencies would question the SEC's "balance."

Furthermore, SIFMA recognizes that this Proposal is one of many rules which the Commission has produced in the past few months—indeed, the Commission is producing rules at the fastest rate since 2011 (which was largely driven by the Dodd-Frank Act).[9] Given the range of Commission activity, SIFMA encourages the Commission to cautiously and carefully deliberate over the Proposal so as not to cause significant market disruptions.[10]

---

[5] Please note that references here to "prudential" regulators are meant to connote agencies with statutory regulatory responsibility over "safety and soundness" or behavioral conduct of companies.

[6] *See* Ben Kochman, *Biden Cyber Officials Pitch Partnership Amid Hacking Threat*, Law360 (Apr. 22, 2022), *available at* https://www.law360.com/corporate/articles/1482974/biden-cyber-officials-pitch-partnership-amid-hacking-threat.

[7] The Proposal at 25.

[8] *See e.g.*, *Critical Infrastructure Partnerships and Information Sharing*, CISA, *available at* https://www.cisa.gov/critical-infrastructure-partnerships-and-information-sharing.

[9] *See* Kenneth E. Bentsen Jr., *Too much, too quickly from the SEC*, THE HILL (Apr. 15, 2022), *available at* https://thehill.com/opinion/finance/3267550-too-much-too-quickly-from-the-sec/.

[10] Given the complexity of the Proposal and the significance of any rules ultimately adopted by the Commission, SIFMA believes that this short comment period is not adequate to fully analyze and respond to the Proposal. *See Joint Comment Letter from SIFMA and other associations to the Commission on the "Importance of Appropriate*

Given the undeniable importance of cybersecurity issues, SIFMA recommends that the SEC should better harmonize and integrate its proposed requirements with extensive existing or in-process strategic cybersecurity laws, rules, regulations and authoritative recommendations, including the Cyberspace Solarium Commission (Bi-partisan US National Strategy),[11] Presidential Executive Order on Improving the Nation's Cybersecurity,[12] the Cyber Incident Reporting for Critical Infrastructure Act (designating CISA as the central place for US government cybersecurity incident reporting and handling),[13] and various prudential regulatory requirements and data breach notification laws throughout each of the 50 United States and various territories.

The SEC should also be mindful that many registrants are obligated to work with international cybersecurity counterparts to CISA and the Federal Bureau of Investigation ("FBI"), and are subject to complying with global non-public, incident-reporting regulations. The Proposal's "balance" simply does not take account of this elaborate web of cybersecurity interaction that takes place – behind the scenes – during a significant cyber event or incident.

If the SEC determines to move forward with this Proposal, SIFMA recommends that this guidance should incline toward clearer examples that take into account the various factors the SEC expects companies to weigh in assessing materiality, and should accord greater respect to the myriad other cybersecurity obligations to which public companies are subject. In these circumstances, SIFMA respectfully requests that the Commission issue a revised notice of proposed rulemaking that is properly aligned with these principles before proceeding to a final rule.

I. Executive Summary

SIFMA believes the Commission should reconsider its proposal in light of the following:

- The Commission is not a prudential cybersecurity regulator for all registrants. The Commission should receive input on the Proposal from prudential cybersecurity regulators. The Commission should more thoroughly consider how it will effectively harmonize and collaborate with prudential regulators, as well as the CISA, the FBI, the Department of Justice ("DOJ"), and relevant foreign counterparts, to best support the relevant interests of investors, registrants, critical infrastructure, law enforcement and national security.

- The Commission should evaluate and respect the deleterious impact its Proposal could have on the public-private partnerships necessary to defend the nation's cybersecurity. The Administration and U.S. cybersecurity agencies have repeatedly, publicly invoked that such collaboration is an absolutely essential component of our national cybersecurity strategy. For example, if a company is actively working with CISA, the FBI, and the

Length of Comment Periods", SIFMA (Apr. 5, 2022), *available at* https://www.sifma.org/resources/submissions/importance-of-appropriate-length-of-comment-periods.

[11] *Cybersecurity Solarium Commission, available at* https://www.solarium.gov/ (last visited May 9, 2022).

[12] Executive Office of the President, *Improving Nation's Cybersecurity*, 86 FR 26633 (May 17, 2021).

[13] Cyber Incident Reporting for Critical Infrastructure Act of 2022, H.R. 2471, 116th Cong. (2022).

Treasury Department on a live cybersecurity threat, should public reporting to the SEC take precedence over collaboration with these agencies, or alternatively, should such collaboration "justify [] providing for a reporting delay"? SIFMA respectfully suggests that such cybersecurity agencies might appreciate a reporting delay to combat serious cyber risks effectively and responsibly.

- The four business day reporting requirement for material cybersecurity incidents, without needed exceptions, may substantially harm both investors and registrants. While we understand the four business day reporting requirement is the standard for all 8-K updates, other 8-K filings are typically less complex than an ongoing cybersecurity incident and do not put registrants at risk like a cyber filing would. Specifically, such reporting requirements may impede necessary and essential internal investigations or cooperation with U.S. law enforcement or national security agencies (and their foreign counterparts). Additionally, this rigid timeline may cause registrants to publicly disclose information before they have a complete understanding of the incident, and such public disclosure may result in investor confusion and unwarranted stock impacts. For example, premature or disproportionate reporting of incidents could imply a materiality that is promptly abated by successful incident response, effective mitigation or remediation, or sufficient business resiliency protocols and resources, or later determined to have not been material in the first instance. Moreover, the four business day deadline to disclose after determining materiality will tend to incentivize registrants to err on the side of over-reporting – i.e., lowering the proper threshold for materiality determinations. If this timeframe were retained, then exceptions are needed, for example, for ongoing investigations and cooperation with law enforcement or cybersecurity agencies. The Proposal may initiate premature public disclosure of cyber incidents and incident details which will have a significant likelihood of interfering with and damaging US national security, especially if release of this information is related to a nation state attack and is not coordinated with the appropriate prudential cybersecurity agencies and regulators.

- Premature, disproportionate and overly prescriptive public disclosure of cybersecurity incidents, and cybersecurity risk management practices and governance risks, will inevitably harm registrants without providing benefits to investors. Disclosure could tip off malicious actors to thematic vulnerabilities within the affected company or within companies throughout the financial sector, especially if an incident has not been fully remediated. This risk is compounded if the SEC further requires detailed disclosures about relevant supply chains.

- The proposed guidance and examples related to the materiality standard are unduly subjective and overly vague. The Proposal seems to presume (without substantiation) that there is currently systematic under-reporting of material cybersecurity incidents to investors. Specifically, the examples of material cybersecurity incidents in the Proposal imply an overly broad approach to materiality. The Proposal could result in registrants over-reporting on cybersecurity incidents, thereby eroding the concept of "materiality."

- The Commission's reporting requirement also conflicts with both Federal and State data breach notification laws and could merely add another confusing compliance burden to registrants that provides minimal benefit to investors. At the very least, the SEC should

reconcile its reporting requirements with applicable data breach notification laws so that public disclosure to investors does not occur before companies complete appropriate investigations and analysis to comply with such laws.

- The Proposal's board and governance disclosure requirements could cause management to look to SEC reporting standards for applicable cybersecurity standards instead of focusing on what prudential regulators and cybersecurity agencies require or recommend.

- Appointing a cybersecurity expert to a registrant's board of directors is not necessarily the best or only way to advance the oversight of a board as a deliberative body. Additionally, this may be difficult for differently sized registrants, especially considering the lack of availability of recognized experts and the difficulties and costs of finding such experts. This could be misleading to investors because a company without specific board experts in cybersecurity may have an extremely knowledgeable CISO and information security staff. In addition, the SEC should avoid directing public companies to seek out single-focus directors.

- The costs of compliance with the Proposal will include diversion of resources and diffusion of focus away from compliance with and implementation of cybersecurity practices that are actually required of or appropriate for public companies in different sectors and with different cybersecurity risk profiles. Moreover, the Commission should revise its economic analysis of the Proposal based on the comments it receives so as to more accurately describe the benefits to investors, costs to registrants, and heightened cyber risks to companies, the economy and national security.

II. The Proposal Would Establish the SEC as a Cybersecurity Regulator for Public Registrants and Exceed the SEC's Authority; the SEC Role Should Be Confined to What Is Strictly Relevant to Investment Decisions.

a. The Appropriate Cybersecurity Regulators

We applaud the SEC for recognizing that cybersecurity risks, mitigation strategies, and frameworks are critical to management and investors of nearly all public registrants. However, the SEC should proceed with caution and refer to existing rules, guidance, regulators, cybersecurity agencies and consumer protection authorities. ***While the Commission is a prudential regulator for broker-dealers and registered investment advisers, it is not so for registrants with respect to cybersecurity, or otherwise.*** As recently discussed by Chair Gensler, the SEC has a role to play with respect to cybersecurity, but "[o]ther government entities, such as the [FBI] and CISA, captain Team Cyber."[14] The Commission should collaborate with and defer to other agencies to avoid disrupting the collaborative cyber effort.

[14] Chair Gary Gensler, *"Working On 'Team Cyber'" - Remarks Before the Joint Meeting of the Financial and Banking Information Infrastructure Committee (FBIIC) and the Financial Services Sector Coordinating Council (FSSCC)*, SECURITIES AND EXCHANGE COMMISSION (Apr. 14, 2022), *available at* https://www.sec.gov/news/speech/gensler-speech-joint-meeting-041422.

For example, public registrants in the financial sector are already and soon will be subject to yet further cybersecurity requirements from a formidable array of regulators, regulations and strongly recommended guidance. Below is just a partial sample of representative cybersecurity regulations applicable to registrants that are financial institutions. The SEC does not need to add to this myriad of regulations simply to enlarge its role in this space for public companies generally.

For instance, SIFMA members already respond to or are regulated by the following U.S. agencies (or their foreign counterparts) on matters related to cybersecurity, including: CISA; Commodity Futures Trading Commission; FBI; the Federal Financial Institutions Examination Council ("FFIEC"), and Federal Bank Regulators such as the Department of the Treasury, Federal Reserve System, Federal Deposit Insurance Corporation, National Futures Association, New York Department of Financial Services (specifically through its Cybersecurity Regulation), and Office of the Comptroller of the Currency. Additionally, insurance company members are also regulated by insurance regulators in each state and territory where they are licensed to do business. And, of course, the SEC is also a prudential regulator for certain financial institutions in their capacities as broker-dealers or as other SEC-registered entities (and the Commission has only recently proposed new rulemaking in that capacity). Moreover, numerous SIFMA members may be considered critical infrastructure subject to specific regulations—SIFMA recommends the Commission harmonize its rules to ensure they do not conflict with security incident reporting requirements for critical infrastructure.

b. **The Commission Should Collaborate and Coordinate with Prudential Cybersecurity Regulators to Ensure the Proposal Does Not Conflict With Any Existing or Upcoming Regulations**

The last few years has seen a preponderance of legislation and regulatory requirements, many of which are upcoming. President Biden signed an Executive Order on May 12, 2021, on Improving the Nation's Cybersecurity, which primarily focused on improving federal agencies cybersecurity defenses, as well as improving the cybersecurity of the supply chain. Congress recently passed the Cyber Incident Reporting for Critical Infrastructure Act, which will require critical infrastructure entities to report material cybersecurity incidents and ransomware payments to CISA within 72 and 24 hours, respectively.[15] CISA must promulgate a proposed implementing regulation within 24 months from final enactment date of March 15, 2022, and a final regulation no later than 18 months thereafter. The Act also calls for harmonization of cybersecurity reporting that would help avoid counter-productive and burdensome conflicts and redundancy.

SIFMA recommends that the Commission focus on eliciting high-level rather than granular information from registrants concerning the cyber regulation and standards to which they are subject and how they address such obligations, as well as what genuinely material cyber risks they have faced and are likely to face.

[15] As drafted, the reporting requirements will cover multiple sectors of the economy, including chemical industry entities, commercial facilities, communications sector entities, critical manufacturing, dams, financial services entities, food and agriculture sector entities, healthcare entities, information technology, energy, and transportation.

"Material" should represent a reasonably high threshold, not a commonplace one. By proliferating additional cybersecurity standards and reporting requirements, registrants and investors will be confused, and registrants that are the victims of cybercrime or other cyber-attacks will inevitably have to address another layer of investigation by a division of an agency whose expertise and responsibility are not, and should not be, focused on cybersecurity. SIFMA encourages the Commission to collaborate with other agencies working in this area so as not to risk requiring duplicative or misplaced efforts from registrants. SIFMA also recommends that the Commission consider providing certain safe harbors from additional reporting requirements, or forbearance, for industries that are already heavily regulated with respect to their substantive cybersecurity and data protection practices and disclosure requirements. At a minimum, the Commission should explain and justify how it harmonizes its Proposal with, and defers to, the work of agencies that are authorized to regulate or provide guidance on cybersecurity.

The Commission should acknowledge that cybersecurity regulation of registrants is outside the primary competency and authorization of the Division of Corporation Finance and that detailed cybersecurity regulation of registrants will cause undue proliferation of cyber standards and will be confusing, burdensome and ultimately counter-productive. Additionally, the Commission should recognize that FINRA and Division of Exams have existing responsibilities related to cybersecurity and information security and do so through periodic examinations outside of the public company context.

c. The Appropriateness of Disclosures.

i. Granular Public Disclosures May Lead to Investor Confusion, Market Volatility, and Security Risks

Disclosures in public filings should not be an avenue for substantive cybersecurity regulation. This Proposal risks misalignment of responsibility. The Proposal may not protect the orderliness of the markets and public confidence in the market system. For instance, public companies should not learn about third-party security incidents from the service providers' SEC filings (as opposed to directly from their own service providers). By displacing existing data breach and cybersecurity incident reporting requirements, the Proposal may disrupt proper business-to-business reporting relationships.

Additionally, the proposed use of the SEC's prescribed disclosure forms is procrustean, and may lead to further confusion. Standardized forms can lead to confusion by including character limits for certain questions or only providing drop down menus with limited options. ***Forcing cybersecurity disclosures into pre-assigned forms could result in one-size distorting all. Flexibility is inherently necessary and appropriate for the broad diversity of businesses, capabilities, strategies, threats and risks faced by different companies.*** Registrants should have the flexibility to describe their cybersecurity disclosures in the manner that fits their profiles, rather than standardizing disclosure. Moreover, requiring excessive or specified granular detail could make for misleading or unhelpful boilerplate.

Public disclosure of granular information could also lead to heightened security risks. Disclosure could tip off other malicious actors to thematic vulnerabilities within the affected

company or within companies throughout the financial sector, especially if the incident has not been fully remediated.

ii. The Commission Should Consider a More Flexible Method for Public Disclosures

SIFMA recommends the Commission consider a less rigid response. At a minimum, SIFMA recommends that the Commission tighten certain definitions and drop vague references, which will promote clarity for compliance obligations. For instance, the definition of Cybersecurity Incident is too broad, and the list of examples in the Proposal may illustrate a threshold that is too low. The current definition of Cybersecurity Incident as an occurrence that "jeopardizes" a registrant's information systems or information, as opposed to an occurrence that has an actual impact on such systems or information, is simply too expansive, and could capture potential events that do not and likely will not actually result in significant, negative ("material") impact to the registrant. SIFMA recommends the Commission provide further clarity to narrow this definition.

The number of different, separate disclosures required by the Proposal is also unreasonable. It cannot be justified under the Paperwork Reduction Act – especially in light of myriad other existing cybersecurity disclosure and reporting obligations.[16] We recommend the Commission reexamine and re-issue its Paperwork Reduction Act analysis in light of the comments provided here. Specifically, the amount of information the Proposal would require to be produced is unwarranted in light of other, existing regulations and the Commission's lack of statutory responsibility for cybersecurity regulation of public companies.

iii. Public Disclosures May Give Rise to Unwarranted Liability and Risk

Additionally, required disclosures may expose registrants to excessive, unwarranted securities litigation or potential enforcement every time they are attacked by cybercriminals or state-sponsored threat actors regardless of whether there is any actual material impact or fault on the part of the registrant, and constrain companies' ability to defend themselves properly against legal challenges. Unrefined and indiscriminate piling on of legal risks in the realm of cybersecurity is in the interest of neither registrants nor their investors.

In general, enforcement against companies that are the victims of cyber-attacks should be the province of prudential regulators or consumer protection authorities, not via collateral litigation or securities law enforcement. Prudential regulators or consumer protection authorities are in the best position to evaluate the sufficiency of a company's cybersecurity safeguards and

[16] While the Proposal purports to conduct a Paperwork Reduction Act analysis, its calculation of costs and benefits is skewed. Different but overlapping disclosure and reporting requirements do not correlate with lower burdens on information providers, but rather, escalated burdens and costs. And if the overlapping requirements conflict or confuse, the resulting benefits to information recipients can be non-existent or negative. Also, while not directly addressed in the Proposal, SIFMA respectfully notes that cybersecurity enforcement-type or educational "sweeps" conducted by the SEC to elicit information about cybersecurity risks and practices must also comply with the Paperwork Reduction Act, and receive requisite advance approval from the Office of Management and Budget's Office of Information and Regulatory Affairs.

efforts relative to the risks they face. Additionally, prudential regulators and law enforcement are the best positioned to assist registrants in pursuing bad actors.

d. Existing SEC Guidance Is Already Reasonably Effective and Could Be Sufficient with Some Updating and Limited Additional Elaboration.

A rule as granular and prescriptive as the Proposal is not necessary and SIFMA encourages the SEC to instead build off its current guidance in this area. For example, in 2020, the Office of Compliance Inspections and Examinations ("OCIE"), renamed now the Division of Examinations, published exam observations that discuss several industry practices, including governance and risk management; access rights and controls; data loss prevention; mobile security; incident response and resiliency; vendor management; and training and awareness.[17] Additionally, in 2018, the SEC published a Release titled "Commission Statement and Guidance on Public Company Cybersecurity Disclosures," which emphasized a range of factors that may affect whether an incident should be disclosed to investors beyond the bottom-line financial costs to respond to the incident.[18] Also in 2018, the SEC released an investigative report on business email compromises, which cautioned public companies to consider cyber threats when implementing internal accounting controls.[19]

SEC enforcement also provides a relevant guide for registrants. For instance, the SEC charged the entity formerly known as Yahoo! Inc. for misleading investors by "failing to disclose one of the world's largest data breaches in which hackers stole personal data relating to hundreds of millions of user accounts."[20] The Yahoo! settlement in particular has provided some guidance to registrants about what sort of public company breaches were subject to SEC jurisdiction. As stated in the SEC's press release, "Yahoo's failure to have controls and procedures in place to assess its cyber-disclosure obligations ended up leaving its investors totally in the dark about a massive data breach. Public companies should have controls and procedures in place to properly evaluate cyber incidents and disclose material information to investors."[21] Finally, the SEC frequently publishes alerts on cybersecurity, such as the Division of Examinations which published three related alerts in 2020 (OCIE Cybersecurity and Resiliency Practices; Ransomware Alert; and Safeguarding Client Accounts against Credential Compromise). Rather than implement a detailed, overweening new Proposal, the SEC can build off these existing guides and best practices.

---

[17] *See Cybersecurity and Resiliency Observations*, OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS (Jan. 27, 2020), https://www.sec.gov/report/ocie-cybersecurity-resiliency-observations.

[18] *See Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, SECURITIES AND EXCHANGE COMMISSION (Feb. 21, 2018), https://www.sec.gov/rules/interp/2018/33-10459.pdf.

[19] *See SEC Investigative Report: Public Companies Should Consider Cyber Threats When Implementing Internal Accounting Controls*, SECURITIES AND EXCHANGE COMMISSION (Oct. 16, 2018), *available at* https://www.sec.gov/news/press-release/2018-236.

[20] *Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees To Pay $35 Million*, SECURITIES AND EXCHANGE COMMISSION (Apr. 24, 2018), *available at* https://www.sec.gov/news/press-release/2018-71.

[21] *Id.*

III. Incident Reporting Requirements

The Commission's four business day reporting period for material cybersecurity incidents could actually pose risk to registrants and their investors. We recommend that the Commission reconsider the four business day reporting period to align with the specific circumstances, exigencies, regulatory obligations, and investigative needs applicable to any given incident. A specific timeframe for public disclosure is simply misguided. If incidents are truly material, perhaps an argument can be made that investors should know about breaches before impacted data subjects, but in general, experience suggests that is unnecessary and may be inappropriate. Additionally, we recommend the Commission revise the incident reporting form to only include a general description of an incident's high-level details to the extent needed to convey the material parts of the incident, such as the basic nature, scope and impact of the incident and avoid mandating or suggesting an SEC "format" for incident reporting (e.g., Item 1.05). Numerous federal, state and international data breach notification and cybersecurity event reporting statutes already exist – and the Securities Exchange Act of 1934 is not one of them.

a. Item 1.05 Should Not Require Public Disclosure of Remediation Details. Request for Comment 1.

A rigid four-business day reporting requirement may go against the principles of responsible disclosure. Responsible disclosure entails holding off on public disclosure until the responsible parties have been allowed sufficient time to patch or remediate the vulnerability or issue. This is particularly important for financial institutions and other critical institutions. Victims of significant cyber breaches must be able to focus on mitigating the incident without the additional pressure of prematurely stimulating market volatility or exposing themselves to additional risk prior to full remediation of the vulnerability. Under the Commission's current Proposal, registrants would be required to publicly disclose certain incidents that are still in the process of being remediated or that may also impact other registrants that have not yet been notified or had time to investigate or remediate. ***We recommend the Commission remove (5) from Item 1.05—registrants should not be forced to disclose details of remediations, and registrants should only publicly disclose such information after the incident has been fully investigated and remediated.***

We also note that requiring disclosure prior to full remediation may signal to the current threat actor or other bad actors that the registrant continues to have a vulnerability that can be further exploited and may otherwise jeopardize internal remediation efforts. Disclosure prior to remediation may also make the registrant more susceptible to other attacks: while the registrants' resources are focused on remediating the disclosed issue, the malefactor or other bad actors may look to attack the registrant's environment more broadly in the hope of identifying other vulnerabilities to exploit.

Requiring public disclosure prior to fully implementing remediation risks unintended adverse impacts to shareholders and the markets. Such premature notification may cause shareholders to withdraw their investment from the company, even in situations where the company believes that effective remediation would mitigate the overall risk of the cyber incident

without material adverse impact on the business. Requiring premature disclosure could therefore add to undesirable market volatility and prompt unwarranted securities litigation.

b. The Proposal's Incident Reporting Requirements on Form 8-K Are Unnecessarily Prescriptive and May Impede Internal Investigations of Cyber Incidents and Events that Registrants Routinely Must Conduct. Request for Comment 3, 4, 7

i. Four Business Days May Be Insufficient Time to Fully Investigate and Publicly Disclose a Cybersecurity Incident

The Proposal acknowledges but does not adequately respect the need of registrants to dedicate essential, necessary time to investigate in order to understand and mitigate or remediate incidents, and to work collaboratively with law enforcement, prudential regulators, cybersecurity agencies, national security agencies, and other necessary entities. During an incident investigation, a registrant's understanding of the incident naturally evolves. Disclosing an incident quickly could cause inadequate or unreliable reports to be filed, which should not yet be relied upon, and which could lead to media and other questions that distract from core incident response and remediation efforts, as well as investor confusion. Further, the detailed requirements for disclosure will make updates and corrections more likely, creating potential investor confusion, which could undercut the SEC's mission of ensuring orderly markets. The Proposal provides some helpful guidelines and flexibility for reporting material cybersecurity incidents. However, requiring registrants to report material cybersecurity incidents four business days after determining the incident is material may add an unnecessary burden on these registrants as they deal with an ongoing incident. The first few days of a cybersecurity incident are crucial. In a real-world scenario, such as the NotPetya cyber-attacks in June 2017, impacted companies may only know that systems have gone offline, and may be struggling to stay afloat, within the first four business days after an incident. Reporting the incident publicly before an investigation is fully underway and before relevant facts can be gathered and impacts assessed could be devastating for a company under those circumstances, and in the case of financial institutions, could even lead to scenarios such as bank runs.

The proposed real-time and after-the-fact reporting of cybersecurity incidents will have unintended consequences such as a distraction of time and resources from the registrant's actual response, as well as a signal to the threat actors about the registrant's level of knowledge related to the incident. Requiring registrants to fill out a standardized form in four business days—when they are perhaps undergoing real-time incident response and do not have all facts in place—would not only place an undue administrative burden on these registrants, but would also open registrants up to civil and criminal liability for misrepresentations made when a company *knows* that it is not in possession of all relevant facts.

Additionally, as discussed by Commissioner Peirce's Dissenting Statement, the Proposal does not consider the need to cooperate with, and sometimes defer to, the federal government and state government. Ongoing governmental investigations (or remediation or disruption efforts) may need to stay confidential for a certain period of time and doing so could increase the chances of recovery of stolen funds or prevention of additional wrongdoing.

ii. The Commission Should Consider Exceptions to the Four Business Day Reporting Requirement for Material Cybersecurity Incidents

The SEC acknowledges the importance of cooperation with law enforcement by companies impacted by cybersecurity incidents but has not allowed for delayed reporting because of a company's cooperation with law enforcement. This exception is a must-have, and not having it means a company that has already been impacted by a cyber attack will be forced to choose between jeopardizing criminal or national security investigations that may have dire national implications or suffering the consequences of not complying with the SEC's rules. Publicly disclosing information that law enforcement or regulators could utilize in an investigation could impede the proper course of the investigation and cause unintended consequences, such as revealing sensitive information upon which bad actors might act. And this is at a time where law enforcement is striving to improve disclosure and collaboration with impacted companies in order to better protect U.S. companies and individuals and to catch cyber criminals and other malicious actors. Other regulators with strict reporting deadlines do not publicly disclose information related to ongoing investigations. Indeed, other agencies that request information on security incidents, such as CISA and the FBI, have stressed that they do not share breach report data with regulatory agencies such as the FTC or SEC.[22] ***Significantly, companies may receive court orders that prohibit any disclosure, including of course public disclosure, of cybersecurity incidents in order to allow government agencies time to obtain evidence and even to plan and execute technical operations to disrupt malicious cyberattacks.***[23]

Form 8-K and Item 1.05 should include an exception to the reporting time where disclosure of a cyber incident or vulnerability could have a more damaging effect than delayed disclosure. For example, if a company discovers it has been impacted by a zero-day vulnerability in widely used software, and the company is required by the SEC to report it publicly, before allowing sufficient time for a patch or other remedial measures to be put in place, other companies will be caught on a backfoot, while bad actors are able to exploit the vulnerability across multiple companies.[24] Such a "responsible disclosure" exception would allow vendors a reasonable opportunity to develop a patch so that other companies could harden their cyber defenses and eliminate the possibility that a report under this regime could alert hackers to an unpatched weakness and lead to a more widespread harm than otherwise would have been experienced.

---

[22] *See* Ben Kochman, *Biden Cyber Officials Pitch Partnership Amid Hacking Threat*, Law360 (Apr. 22, 2022), *available at* https://www.law360.com/corporate/articles/1482974/biden-cyber-officials-pitch-partnership-amid-hacking-threat.

[23] *See Justice Department Announces Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate (GRU)*, DEPARTMENT OF JUSTICE (Apr. 6, 2022), *available at* https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-botnet-controlled-russian-federation.

[24] *See CISA COORDINATED VULNERABILITY DISCLOSURE (CVD) PROCESS*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, *available at https://www.cisa.gov/coordinated-vulnerability-disclosure-process* (last visited May 9, 2022).

c. Public Disclosures of Cybersecurity Incidents May Have Severe or Significant Detrimental Security Implications. Request for Comment 1, 2, and 3

The Proposal would require registrants to reveal sensitive information concerning material security incidents—many of which may be ongoing incidents. Malicious threat actors will undoubtedly use this information, and could stand to benefit from it in many ways:

(1) If a threat actor is engaged in attacking a registrant, and it notices that the registrant has not notified the SEC, the threat actor may infer that it has not been detected and will use that information accordingly.
(2) If a threat actor is engaged in attacking a registrant, and it notices that the registrant has notified the SEC, it will monitor the release to learn how much the registrant knows of the incident. The threat actor may choose to immediately exfiltrate data if it knows it has been identified and its presence in a system may soon be remediated. Conversely, the threat actor may leverage separate attacks if it learns that the registrant does not completely understand the scope of the attack or has not mitigated the attack.
(3) If a registrant publicly discloses an ongoing attack by a threat actor, other threat actors may monitor the publicly available information and target the registrant as well.
(4) If a registrant publicly discloses that a material incident has not been remediated (or is in the process of being remediated), threat actors will exploit this vulnerability.

Disclosing individually immaterial cybersecurity incidents which have become material in the aggregate will also have potentially negative consequences. Many of these disclosures may provide a road map to threat actors for how to continue to exploit a vulnerability, and it is best to wait to properly disclose until after the vulnerability has been remediated.

Under the current Proposal, registrants would have to disclose the details of material cybersecurity incidents within four business days, even if the registrants are unable to mitigate the vulnerability themselves or have limited information. Upstream vendors could be the source of a material security incident, and the registrant may be unable to fix the issue until the vendor has remediated it. Registrants may be largely dependent on vendors to provide information in these circumstances.

The Commission should consider removing (1) and (3) from Item 1.05. For purposes of informing shareholders, the disclosure should only include a brief description of the incident and the effects (if any) on the registrant's operations. More detailed information, especially for an ongoing incident, will complicate incident response, increase potential liability (with respect to attackers and from a legal standpoint), and lead to more public relations efforts on the part of the registrant that suffered the incident without clearly providing additional benefits to investors. The types of information the SEC states it would not expect a company to disclose should include information related to a company's cyber insurance policies, because malicious actors, particularly ransomware attackers, look for this type of information to craft ransom demands.

d. The Proposed Materiality Standard Is Unduly Subjective and Vague and Could Result in Registrants Being Held Unfairly Accountable to a Standard that Only *Appears* to Be Objective or Precise. Request for Comment 5, 8, and 12.

i. The Proposal Lacks Clarity on What Constitutes a Material Cybersecurity Incident – and Does Not Take Adequate Account of Available Resiliency and Recovery Mitigations

Only material cybersecurity events should be publicly reported, but there is currently a lack of clear explanation on how to make this determination as it relates to cybersecurity incidents. Although the Commission does discuss the definition of materiality, the Proposal is unduly subjective and vague as to what types of incidents could rise to the level of materiality and under what circumstances. It is rare that a cybersecurity incident is immediately obvious as material – especially where cybersecurity programs now stress resiliency and recovery in addition to prevention. ***The Proposal provides various qualitative dimensions to consider in determining the materiality of a cybersecurity incident, but the Proposal lacks concrete thresholds to assist registrants in determining materiality. Lack of clarity could lead to investor confusion over how to discern between the impactful security incidents from the non-impactful security incidents.*** Some internal cyber events, including even data loss, impacting IT systems may be potentially consequential to companies, but would not necessarily be material provided that companies effectively mitigate through remediation, back-ups and resiliency. Companies should be permitted to make their own determination of incidents that rise to the level of notification—and these considerations should include ensuring that any publicly disclosed information does not put the registrant at further risk. If not, the Commission should consider a quantifiable threshold for materiality that would be similar to other financial losses for materiality determinations.

The Proposal provides a non-exclusive list of examples of cybersecurity incidents which, if deemed material may trigger incident disclosure. For reference, the list includes the following examples:

- An unauthorized incident that has compromised the confidentiality, integrity, or availability of an information asset (data, system, or network); or violated the registrant's security policies or procedures. Incidents may stem from the accidental exposure of data or from a deliberate attack to steal or alter data;
- An unauthorized incident that caused degradation, interruption, loss of control, damage to, or loss of operational technology systems;
- An incident in which an unauthorized party accessed, or a party exceeded authorized access, and altered, or has stolen sensitive business information, personally identifiable information, intellectual property, or information that has resulted, or may result, in a loss or liability for the registrant;
- An incident in which a malicious actor has offered to sell or has threatened to publicly disclose sensitive company data; or
- An incident in which a malicious actor has demanded payment to restore company data that was stolen or altered.

This list comprises types of incidents that if well managed through effective incident response and remediation, would not necessarily constitute a material cybersecurity incident. Indeed, many SIFMA members have protocols in place which would mitigate the negative consequences of many of the listed examples. For instance, many SIFMA members, as well as other registrants, carry cybersecurity insurance that will provide coverage for financial losses as a result of a cybersecurity incident. Moreover, the four business day deadline to disclose after determining materiality will tend to incentivize registrants to err on the side of over-reporting and lower the proper threshold for materiality determinations. We recommend the Commission clarify that registrant's traditional assessments concerning materiality (including available mitigation), and analysis thereof, will continue to apply.

ii. Other Prudential Cybersecurity Regulators Have Prescribed Definitions of Security Incidents and Carry the Risk of Public Disclosure

The Proposal's examples of security incidents are broad and vague and should be clarified. Several prudential cybersecurity regulators have narrowly defined examples of significant security incidents with correspondingly high thresholds. Importantly, these regulators will not publicly share the details of such disclosures. For instance,

- The newly passed Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA") will require reporting of a "significant cyber incident, or a group of related cyber incidents … likely to result in *demonstrable harm* to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the people of the United States."[25]

- The Department of the Treasury, Federal Reserve System, and Federal Deposit Insurance Corporation recently announced a final rule requiring banks to notify their primary regulator of any significant computer-security incident "that *disrupts or degrades, or is reasonably likely to disrupt or degrade, the viability* of the banking organization's operations, result in customers being unable to access their deposit and other accounts, or *impact the stability of the financial sector*."[26]

  The New York Department of Financial Service's ("DFS") Cybersecurity Regulation defines a cybersecurity event as "any act or attempt, whether successful or not, to gain unauthorized access to, disrupt, or misuse an information system or information stored on such system."[27] DFS requires reporting of Cybersecurity Events if the event falls into one of two categories: (1) the Cybersecurity Event impacts the Covered Entity and notice of it is required to be provided to any government body, self-regulatory agency or any

[25] Cyber Incident Reporting for Critical Infrastructure Act of 2022, Section 2240(16)(emphasis added).
[26] *See Final Rule: Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, available at* https://www.occ.treas.gov/news-issuances/news-releases/2021/2021-119a.pdf *(emphasis added).*
[27] *See Cybersecurity Resource Center,* NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES, *available at* https://www.dfs.ny.gov/industry_guidance/cybersecurity (last visited May 9, 2022) (emphasis added).

other supervisory body; or (2) the Cybersecurity Event has a reasonable likelihood of *materially harming any material part of the normal operation*(s) of the Covered Entity.[28]

iii. Registrant's Public Disclosure of Cybersecurity Incidents May Cause an Unwarranted Negative Impact on a Stock's Price

According to the latest data breach report by IBM and the Ponemon Institute, the average cost of a data breach in 2021 was $4.24 million.[29] The costs of a cybersecurity incident of course vary—and several SIFMA members have compensating controls in place to protect against the Commission's listed examples. Indeed, security incidents do not necessarily, or predictably, cause significant impact on the price of a registrant's stock.

Because the Proposal's definition of materiality is so vague, it will incentivize over disclosure, and disclosure to the SEC and the public may be the only event that causes a negative impact on the stock's price. Additionally, criminal groups may exploit price impacts of data breaches that they cause based on their belief that SEC reporting requirements will result in public disclosures of cybersecurity incidents even if they are not really material.

e. The SEC's Proposal Conflicts with Federal, State and International Data Breach Notification and Cyber Event Reporting Laws – Both in Timing and Substantive Standards; the Disconnect Between Disclosures to Impacted Data Subjects and Investors May Be Problematic. Request for Comment 6.

The reporting requirements under the proposed rule are not aligned with other federal, state, and international cybersecurity incident reporting requirements. The explicit lack of a law enforcement (and national security and cybersecurity agency) exemption is concerning and could undermine national, corporate, and personal security interests. It is also inconsistent with existing cyber notification requirements that do allow for such exemptions. Each Registrant has a number of obligations under either federal or state law in the case of a security incident. The Proposal may add another compliance burden – with a significantly shorter period of time than most other regulations to report the incident to the Commission. The Commission should consider aligning its reporting obligations with other state and federal laws.

f. Updates to Previously Disclosed Cybersecurity Incidents and Previously Immaterial Cybersecurity Incidents Present an Inherent Risk.

Under the Proposal, registrants would be required to provide additional reports where material changes, additions, or updates have occurred with respect to a cybersecurity incident. However, the comments include statements, such as a "description of remedial steps [a company] has taken, or plans to take," in response to the incident.[30] In many cases, that will not be a material change or update and should not require additional reporting. Such a report may also be contrary to the SEC's statement that in an initial 8-K filings related to a cybersecurity

---

[28] *Id.*

[29] *See How much does a data breach cost?*, IBM, *available at* https://www.ibm.com/security/data-breach (last visited May 9, 2022).

[30] The Proposal.

incident the SEC "would not expect a registrant to publicly disclose specific, technical information about its planned response to the incident."[31] The requirement to update reports should be limited to only significantly new or different information relating to a cybersecurity incident. That determination of materiality should be left to a company's discretion based on the same factors used to determine materiality under previous SEC guidance. The Proposal should also address when updates could stop being made—for instance, at the point which the incident itself is no longer material.

Any updates of ongoing cybersecurity investigations could be misleading. Investigations are complex and dynamic, and a registrant's understanding of information is always evolving. Information around registrant's progress in remediating an incident is also valuable information to any malicious actor. SIFMA is concerned with the requirement to speculate on any potential future material impacts on operations and financial condition given the complex and dynamic nature of cybersecurity incidents. SIFMA does not agree that required reporting on the details of remediation measures is appropriate. In general, these measures should remain internal as the details of remediation may themselves expose areas of vulnerability, and they may not be properly understood by, and could be misleading for, inexpert shareholders or potential investors. Cybersecurity regulatory agencies – not the SEC – should focus on the specifics of remediation.

The proposed addition of Item 106(d)(2) would require a company to disclose when a "series of previously undisclosed individually immaterial cybersecurity incidents become material in the aggregate."[32] ***It is unclear what would constitute a "series of previously undisclosed" cybersecurity incidents.*** For example, if similar types of attacks are conducted against the same company by different actors over the course of a year, or even a longer period, it is not clear if that would be considered a series of cybersecurity incidents. It would also not be clear if the same threat actor conducted multiple attacks over a period of time. Similarly, it may not be clear if different government-linked advanced persistent threats conducted attacks whether it should be considered a series of cybersecurity incidents (*e.g.*, Fancy Bear and Cozy Bear, both of which have been linked to Russia). Material in the aggregate is difficult to define (it has not been explicitly defined by the SEC) and operationally challenging to follow. ***The definition of cybersecurity incident refers to "any information" so this would require potentially reviewing unlimited amounts of data over an indefinite period of time. This lack of clarity could cause a compliance risk of over- or under-reporting.***

And perhaps most significantly, many disclosed cybersecurity incidents do not turn out to be material to investment decisions. The SEC's Proposal should acknowledge that empirical reality.

g. Considerations for Foreign Private Issuers. Comment 38, 39.

The proposed change to Form 6-K will result in a potentially onerous requirements for foreign private issuers and many other in the European Union that are subject to Market Abuse Regulation ("MAR") continuous disclosure requirements to immediately disclose non-public

[31] *Id.*
[32] *Id.*

price sensitive information. The proposed change to Form 6-K implies that all cyber incidents reported under the Proposal are material for US SEC purposes. To minimize potential selective disclosure issues, covered foreign private issuers ("FPI") would be best advised to make the home country and Form 6-K announcements concurrently. As MAR requires immediate announcement, then that determines the timeframe within which FPIs must respond, which is immensely challenging given the likely imperfect information FPIs will have about the incident. US registrants generally have four business days to file an 8-K. So, in this instance the Proposal would operate potentially capriciously for FPIs subject to MAR type home country real time disclosure requirements.

We suggest that the inclusion of material cybersecurity incidents is not made to Form 6-K. If home country rules require immediate disclosure of the incident, then US security holders will receive the 6-K concurrently even without the proposed change.

IV. Disclosure Requirements

Existing SEC guidance should be sufficient to elicit relevant information for investors, and if needed could be supplemented to include principles-based discussion of cybersecurity risk management and strategy. The Proposal seems more in-line with prudential regulators and reach beyond typical SEC disclosure requirements. The Commission should be circumspect about what type of information is being forced into the public domain, which will be available to malicious actors and overly technical for investors.

The requirement for a registrant to provide information about its cybersecurity program should be limited to a brief description of: (1) whether the registrant has a cybersecurity program; and (2) a high-level description of the various components of the cybersecurity program or a reference to the cybersecurity framework employed by the registrant. Detailed descriptions of the components, including for conducting cybersecurity due diligence on vendors, creates an additional burden on companies without a clear benefit to investors or to the effectiveness of a company's cybersecurity program. The Commission should deem it sufficient disclosure for registrants to refer generally to the cybersecurity frameworks they follow, such as ISO 27001 Certification or SOC 2 Reports.

a. Board and Governance Disclosure Requirements Are Unduly Prescriptive, Overbroad and Overinclusive, and Could Deny Companies the Ability to Adopt and Follow Their Own Cybersecurity Strategies, Operating Procedures and Alternative Approaches; Identifying Specific Individuals by Name (Even With SEC's Proposed Safe Harbor) May Deter Qualified Individuals and Invite Unfair Accountability. Request for Comment 17, 20, 26, and 27.

i. The Proposal's Item 106 of Regulation S-K and Item 16J of Form 20-F Create an Undue Administrative Burden on Registrants With Limited Benefit to Investors

The proposal includes requirements for issuers to disclose information such as: the cybersecurity expertise of its board members; the registrant's cybersecurity policies and procedures; whether it employs a chief information security officer; and the interactions of management and the board of directors concerning cybersecurity. This will create an administrative burden and lead to companies designing policies and procedures for purposes of SEC reporting rather than broader compliance goals based on risks specific to an organization. If anything, this could become misleading for investors, because a company can list its policies and procedures which could create a false sense of security for investors, even though the detail about the policies has no bearing on their effectiveness. The Commission should consider general references to implementation of industry standards such as ISO 27001 Certification or SOC 2 Reports as sufficient disclosure.

As discussed by Commissioner Peirce's Dissenting Statement, these disclosure requirements look more like a list of expectations about what issuers' cybersecurity programs should look like and how they should operate. We support businesses' integration of cybersecurity expertise and decision making through their board members and management, as well as other measures in the proposal, but these decisions should be left to businesses. Although it does not seem to be expressly addressed in the Proposal, the SEC should make clear that this disclosure requirement does not require companies to disclose whether they maintain cyber insurance. Malicious actors look for that type of information to tailor cyber-attacks toward particular organizations that are more likely to pay ransom when they carry cyber insurance. Additionally, such policies are relatively new and the ultimate scope of coverage may be uncertain.

ii. **The Proposal's Amendments to Item 407 of Regulation S-K and Form 20-F to Create Prescriptive Public Disclosures of a Registrant's Board of Directors Experience and Involvement in Cybersecurity Will Mislead Investors**

Requiring disclosure of cybersecurity expertise for a member of the board of directors may be difficult for many registrants to implement—especially depending on the size of the registrant. Board of directors are distinct from management, as the board's role is one of oversight whereas management is required to have subject matter expertise. The Proposal fundamentally changes the role of the board of directors in a way that is untenable. The board should have the flexibility to determine its own composition and take into consideration the collective expertise of the board, holistically. Boards are, by design, deliberative bodies and tasked with oversight of numerous risks – ***of which cyber is only one of those risks***. "Special interest" board members are not the best way to advance the oversight of a registrant or of a board as a deliberative and collective body; therefore, the Proposal could undermine this model. Current disclosures required concerning board's business experience should be sufficient to elicit relevant information for investors. SIFMA recommends the commission provide an alternative method of disclosure, such as whether the board of directors engages in regular cybersecurity education sessions or engages with expert advisers on the topic.

Appointing a cybersecurity expert should be an individual judgment for individual companies in light of their structure, sophistication, and relevant risks. There is also a potential sourcing issue – there may be not be sufficient people with cybersecurity expertise and requisite

board skills (in some cases C-Suite level). It is also far from clear that the types of expertise provided as examples (*e.g.*, having a cybersecurity certification or degree) is necessary for effective oversight of cybersecurity matters. This could be misleading and create a false sense of confidence among investors, because a company without board members with cybersecurity expertise may have an extremely knowledgeable CISO and other information security staff. Yet the absence of a board member with specific credentials or past experience may unjustifiably impact the perceived risk exposure of a registrant. The SEC should simply not specify how public companies must go about discharging their cybersecurity responsibilities. ***We recommend the Commission lighten its language on this requirement to ensure that this does not transform into a mandate for every registrant to have a cybersecurity expert on its board.***

The Commission proposes requiring disclosure of any cybersecurity expertise of board members and disclosing the names of those directors with expertise. Disclosing the names of board members with cybersecurity expertise could draw unwanted attention to these board members, including from bad actors (e.g., hacktivists) or litigants, and could thereby discourage board memberships.

b. Public Disclosures Concerning Whether and How Cybersecurity Considerations Affect the Selection and Oversight of Third-Party Service Providers May Have Severe or Significant Detrimental Security Implications.

Public disclosure on whether and how cybersecurity considerations affect registrants' selection and oversight of third-parties should only be provided at a very high level, as detailed information could provide a roadmap to vulnerabilities and thematic, widespread breaches should malicious actors detect patterns of selection. More specifically, we do not have concerns in terms of complying with the SEC's policies and procedures expectations. However, public disclosure should be limited to confirmation that policies and procedures are appropriately applied to third-party selection and ongoing oversight as part of a risk-based framework covering the relationship life cycle. Disclosure should not require detailing the mechanisms, controls and contractual details leveraged to mitigate cybersecurity risks related to providers. This could expose firms and their clients/employees to additional cyber risk – the opposite of what the SEC/regulators are aiming for in building sector resilience. Further, exposing this information could put firms at a competitive disadvantage if information about their outsourcing policies, procedures, and service provider list is disclosed publicly (i.e, made available to competitors). Additionally, companies may have confidentiality agreements in place with such third-parties and would be violating the terms of these agreements if they were to publicly disclose such information. Moreover, CISA, and other cybersecurity agencies and security professionals, mitigate the harm of destructive disclosures by implementing Traffic Light Protocols ("TLP"), which is a set of designations used to indicate expected sharing boundaries to be applied by the recipients of sensitive information.[33] Indeed, the Cybersecurity Information Sharing Act of 2015[34] codifies the confidentiality necessary to enhance, and protect, sharing of cybersecurity threat actors and defensive measures by stating that an "entity receiving a cyber threat indicator or defensive measure from another entity or Federal entity shall comply with otherwise lawful

[33] *See Traffic Light Protocol (TLP) Definitions and Usage*, CISA, *available at* https://www.cisa.gov/tlp.
[34] Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, Div. N, Title I (2015).

restrictions placed on the sharing or use of such cyber threat indicator or defensive measure by the sharing entity or Federal entity."[35]

c. Different Companies Require Different Levels of Cybersecurity Investment and Sophistication. Request for Comment 23 and 35.

As discussed, the topics listed in the proposed governance disclosures come off as expectations. However, all these measures will not be required for all registrants, as each registrant will have a different risk profile. For instance, a registrant that does not collect sensitive information or that exists entirely in a third-party cloud environment may not need all the cybersecurity measures listed in the proposal. On the other hand, a registrant that deals with sensitive information, such as children's data or Social Security numbers, may need additional cybersecurity controls. By creating a one size fits all form, investors may get the wrong impression of the relative risk of certain registrants. ***Accordingly, these required disclosures may negatively impact certain registrants that do not require sophisticated cybersecurity controls and governance, and lead investors to believe such registrants are not well positioned with respect to cybersecurity risk governance.***

Additionally, several types of reporting companies already have different reporting requirements. For instance, Federal Banking Regulators and other agencies require certain registrants to certify cybersecurity compliance regularly. Similarly, many state financial services and/or insurance regulators already require regulated entities certify cybersecurity compliance. The Commission should consider exemptions or tailored reporting requirements for registrants that are regulated by different cybersecurity regulators.

d. Public Disclosures Concerning the Details of a Registrant's Cybersecurity Program may have Severe or Significant Detrimental Security Implications. Request for Comment 21, 22, 28, and 31.

These proposed disclosures may inadvertently lead to cybersecurity incidents. The Proposal may provide threat actors with a "road map" to potential vulnerabilities in registrant's cyber controls and associate information systems. Prior to engaging with a target, threat actors will often use open-source intelligence (OSINT) to learn more about their target.[36] While the proposed cybersecurity disclosures will likely have little impact on investors, they may provide significant intelligence to malicious threat actors. We can foresee threat actors using SEC disclosures to target registrants with unsophisticated cybersecurity programs. For instance, a threat actor may target a company that disclosed it is in the process of implementing cybersecurity policies and procedures, or a company that disclosed that its chief information security officer unexpectedly quit, and the position is currently vacant.

---

[35] *Id.* Sec.104(b)(1)(B).

[36] *See Open Source Intelligence (OSINT)*, CROWDSTRIKE (Feb. 25, 2022), *available at* https://www.crowdstrike.com/cybersecurity-101/osint-open-source-intelligence/.

V. Harmonized Definitions for the SEC's Next Iteration (i.e., a Revised Proposed Rule)

Per footnote 80 of the Proposal, the defined terms "are derived from a number of established sources." While we appreciate the Commission's effort to leverage terms and definitions from established sources, we encourage the Commission to go a step further and directly adopt well-established and industry-accepted terms and definitions from a single source (e.g., National Institute of Standards and Technology or Financial Stability Board[37]) to promote consistency of rule interpretation and disclosure across public companies. Doing so will help registrants reduce the time utilized for internal deliberation over the Commission's terminology when making time-sensitive disclosures.

VI. Proposed Safe Harbor for Information Systems Provided by Suppliers and Third-Parties

The Commission's proposed definition of "information systems" includes systems that are "used" by the registrant, placing an unfair onus on registrants to accurately disclose to investors information possessed by a third party. Many registrants use third parties, such as cloud service providers, and may not have complete visibility into such information systems, and may be subject to intellectual property rights and cybersecurity confidentiality. Incidents and vulnerabilities often entail complex relationships among the relevant parties that constrain information sharing on legal grounds.

We recommend the SEC avoid imposing any reporting requirements with regard to cybersecurity information controlled by third parties.

However, if the SEC were to impose any disclosure requirements dependent on third parties, we encourage the Commission to provide registrants a safe harbor for disclosures related to cybersecurity incidents occurring on or conducted through suppliers and third-party systems, as well as other relevant cybersecurity disclosures related to third-party systems. For instance, the Commission recently included a safe harbor in "The Enhancement and Standardization of Climate-Related Disclosures for Investors" for emissions-related data derived from suppliers and third parties, recognizing "concerns that registrants may have about liability for information that would be derived largely from third parties in a registrant's value chain."[38] Here, a proposed safe harbor would offer registrants protection from legal liability or other penalties when a registrant is given inaccurate or incomplete information from a third-party vendor related to a cybersecurity incident or other information necessary for disclosure. Such a safe harbor may encourage registrants to provide meaningful information for investors without increasing the risk of liability for information received from third-parties.

---

[37] *See Cyber Lexicon*, FINANCIAL STABILITY BOARD (Nov. 12, 2018), *available at* https://www.fsb.org/2018/11/cyber-lexicon/.

[38] *See* The Enhancement and Standardization of Climate-Related Disclosures for Investors, 87 Fed. Reg. 21334 (proposed Apr. 11, 2022) (to be codified at 17 CFR 210, 229, 232, 239, and 249) (providing a safe harbor to registrants from forms of liability under the securities laws given challenges in obtaining activity data from suppliers and third parties).

VII. **Costs of Compliance.**

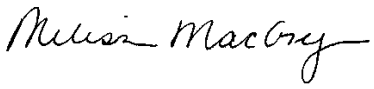
We recommend the Commission account for the relative costs and benefits of this Proposal in light of the inevitable duplication with the regulation and responsibilities of other more expert and relevant agencies. SIFMA members have already substantially invested in cybersecurity compliance and best practices. ***For instance, many SIFMA members have aligned with the NIST Cybersecurity Framework, but the Proposal's lack of alignment and harmonization with NIST or other cybersecurity frameworks may cause SIFMA members to expend substantial resources to reconcile these best practices with the Proposal. This resulting burden and complexity distract cybersecurity professionals from identifying and protecting against the threat environment, and undermines the design of cybersecurity strategies and prioritization of control implementation.***[39] This Proposal will bring limited benefits to investors as well as to SIFMA member's cybersecurity programs, while providing substantial compliance costs to registrants.

*** * ***

SIFMA appreciates the SEC's attention to cybersecurity, and absolutely agrees with the Commission regarding the importance of cybersecurity commitment and resources. However, we respectfully submit the Proposal has mistaken the SEC's proper role on cybersecurity for public companies. The SEC is not and should not seek to become a cybersecurity regulator for public companies, and should focus more narrowly on assuring that investors receive information material to their investment decisions.

Accordingly, SIFMA respectfully urges that the Commission should issue a revised notice of proposed rulemaking in line with its proper, limited role on cybersecurity in the public company context rather than proceed to a final rule. If you have any questions or would like to discuss these comments further, please reach out to Melissa Macgregor at mmacgregor@sifma.org or Thomas Wagner at twagner@sifma.org.

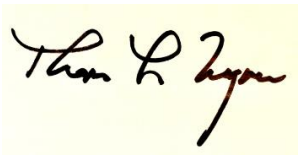
Sincerely,



Melissa MacGregor
Managing Director & Associate General Counsel
SIFMA

---

[39] *See* Financial Services Sector Coordinating Council, *RE: Views on the Framework for Improving Critical Infrastructure Security*, FINANCIAL SERVICES SECTOR COORDINATING COUNCIL (Feb. 9, 2016) ("Industry has a shared concern that the fundamentals of cybersecurity are weakened when, as some firms have reported, approximately 40% of corporate cybersecurity activities are compliance oriented, rather than security oriented. The solution is not merely hiring more cybersecurity personnel as expert staff are becoming an increasingly scarce and costly resource.").



Thomas M Wagner
Managing Director, Financial Services Operations and Technology
SIFMA

cc:
Hon. Gary Gensler, SEC Chair
Hon. Hester M. Peirce, SEC Commissioner
Hon. Allison Herren Lee, SEC Commissioner
Hon. Caroline A. Crenshaw, SEC Commissioner
Renee Jones, Director, SEC Division of Corporation Finance, Director
Kenneth E. Bentsen, Jr., SIFMA President and CEO
Alan Charles Raul, Sidley Austin LLP
Sasha Hondagneu-Messner, Sidley Austin LLP